

## **How to create better passwords - why bother?!** **(2005-12-07 16:43)**

I have recently came across a practical article on [1]how to create a better passwords, courtesy of [2]CSO Magazine.

It reminded me of how many times I find myself actually getting into the science of passwords maintenance and

creation in order to enforce real-life, cost-effective scenarios, while on the other hand, get myself seriously concerned on how **easy it is to have your accounting data abused!**

During the years I have written several articles, like this one - [3]Creating and Maintaining Strong Passwords,

mainly with the idea to actually provide a pragmatic approach on tackling weak, and prone to be cracked passwords.

The result, at least from a sniffing point of view \*grin\* was that most of my friends lacking security knowledge, were

indeed getting concerned by their easy to guess passwords. Later on, they were turning them into entire passphrases

with the idea to avoid not having them cracked. That's an example of a "false feeling of security".

And while it was a progress compared to how predictable their passwords really were, strong passwords doesn't

address the following issues that I later on covered in another article - [4]Passwords - Common Attacks and Possible

Solutions, namely, passwords can be :

- **Sniffed**
- **Recovered**
- **Unintentionally shared**
- **Keylogged**
- **etc.**

Recently, both from a CSO's point of view, and the financial industry, [5]two factor authentication, has been

gaining a lot of acceptance, in my opinion primary because of its tangibility. It greatly improves the authentication

process, given the integrity of the system, and the network itself. And while from an organization's or bank's point

of view providing tokens to the entire work force would represent a huge investment, I strongly feel prioritizing in

respect to important customers, and executives will play an important role.

On October 12, 2005, the [6]Federal Financial Institutions Examination Council, released its [7]Guidance on

Authentication in Internet Banking Environment, thereby enforcing the use of advanced, compared to passwords

based only, authentication approaches.

Would it work? I doubt so, but it limits the age-old attacks we are so used to seeing in respect to passwords.

[8]Bruce Schneier has been discussing the [9]dangers of the two factor authentication buzz, and as far as online

banking is concerned, Candid Wüest has written a very good paper on [10]Today's threats to online banking, namely

the techniques discussed fully apply to any type of authentication. Passwords are out of the topic, even two factor

authentications has its good and bad sides to it comes to end users' awareness, implementation and configuration.

What are the practical alternatives these days?

[11]Password Safe is a bit unpractical(still works for lots of people out there) in today's interconnected world,

namely, a HDD crash for instance would cause a lot of trouble to everyone, let's not mention the "availability" of the 5

data. [12]Just1Key seems to solve this problem to a certain extend. I also recommend you verify the strenght of your passwords by taking advantage of the [13]Password Strenght Meter [14]ComputerWeekly, are also running an

article "[15]Security : have passwords had their day?", they sure haven't, at least not on a large scale, the way I've always wanted to see it - One Time Passwords in Everything! Check out [16]RSA's [17]One-Time Password

Specifications , the concept in itself has the time frame advantage!

Further reading on the topic can be found at :

[18]The Memorability and Security of Passwords - Some Empirical Results

[19]Passwords you'll never forget, but can't recall

[20]One Time Passwords In Everything (OPIE) : Experiences with Building and Using Stronger Authentication

[21]Stealing passwords via browser refresh

[22]A Convenient Method for Securely Managing Passwords

Technorati tags :

[23]passwords,[24]access control,[25]authentication,  
[26]information security,[27]security,[28]identification

1.

[http://www.csoonline.com/read/120105/ht\\_passwords.html](http://www.csoonline.com/read/120105/ht_passwords.html)

2.

<https://web.archive.org/web/20101016193540/http://www.csoonline.com/>

3. <http://www.pcflank.com/art33.htm>

4. <http://www.windowsecurity.com/articles/Passwords-Attacks-Solutions.html>

5. [http://en.wikipedia.org/wiki/Two\\_Factor\\_Authentication](http://en.wikipedia.org/wiki/Two_Factor_Authentication)

6. <http://www.ffiec.gov/>

7. <http://www.ffiec.gov/press/pr101205.htm>

8. <http://www.schneier.com/>

9.

[http://www.schneier.com/blog/archives/2005/03/the\\_failure\\_of.html](http://www.schneier.com/blog/archives/2005/03/the_failure_of.html)

10. <http://www.astalavista.com/index.php?section=directory&linkid=5659>
11. <http://www.schneier.com/passsafe.html>
12. <http://www.just1key.com/>
13. <http://www.securitystats.com/tools/password.php>
14. <http://www.computerweekly.com/>
15. <http://www.computerweekly.com/Articles/2005/12/06/213268/Securityhavepasswordshadtheirday.htm>
16. <https://web.archive.org/web/20101016193540/http://www.rsasecurity.com/>
17. <http://www.rsasecurity.com/rsalabs/node.asp?id=2816>
18. <http://www.ftp.cl.cam.ac.uk/ftp/users/rja14/tr500.pdf>
19. [http://www.cs.huji.ac.il/~kirk/Imprint\\_CHI04\\_final.pdf](http://www.cs.huji.ac.il/~kirk/Imprint_CHI04_final.pdf)
20. <http://chacs.nrl.navy.mil/publications/CHACS/1995/1995mcdonald-USENIX.pdf>
21. [http://www.infosecwriters.com/text\\_resources/pdf/Stealing\\_passwords\\_via\\_browsers.pdf](http://www.infosecwriters.com/text_resources/pdf/Stealing_passwords_via_browsers.pdf)
22. <http://www.cs.princeton.edu/~jhalderm/papers/www2005.pdf>
23. <http://technorati.com/tag/passwords>

24. <http://technorati.com/tag/access+control>
25. <http://technorati.com/tag/authentication>
26. <http://technorati.com/tag/information+security>
27. <http://technorati.com/tag/security>
28. <http://technorati.com/tag/identification>

6

x

x

### **Obay - how realistic is the market for security vulnerabilities? (2005-12-12 16:40)**

In [1]Issue 19 (July, 2005) of the [2]Astalavista Security Newsletter that I release on a monthly basis, I wrote an article entitled " **Security Researchers and your organization caught in between?** " whose aim was to highlight a growing trend, namely the monetization of vulnerability research, who benefits and who doesn't.

A recent, rather significant event at least for me covering and monitoring this issue for quite some time now,

was an Ebay listing for a "[3]brand new Microsoft Excel vulnerability". A bit ironical, but I had a chat with **Dave Endler**, director of security research at [4]**TippingPoint**, and the issue of their future position as bidders for someone else's research were discussed a week before the Ebay's listing in [5]Issue 23 (November, 2005) of Astalavista's Security

Newsletter.

[6]

Two of today's most popular, and at least public commercial entities paying hard cash for security vulnerabilities are :

[7]**iDefense**, and the [8]**ZeroDayInitiative** (TippingPoint).

[9]

But what is the need for creating such a market? Who wins and who loses? What are the future global

implications for this trends, originally started by [10]**iDefense**?

In any market, there are sellers and buyers, that's the foundation of trade besides the actual exchange of

goods/services and the associated transaction. What happens when buyers increase, is that sellers tend to increase

as well, and, of course, exactly the opposite. Going further, every economy, has its black/underground or call it

whatever you want variation. And while some will argue a respected researcher will contribute to the the

development of even more botnets, who says it has to be respected to come with a vulnerability worth purchasing?!

It's a [11]**Metasploit** world, isn't it?!

Going back to the market's potential. Sellers get smarter, transparency is build given more buyers join seeking to

achieve their objectives in this case, provide proactive protection to their clients only, and build an outstanding,

hopefully loyal researchers' database. These firms, to which I refer as buyers have happened to envision the fact

that there are thousands of skilled vulnerability researchers', who are amazingly capable, but aren't getting a penny

out of releasing their vulnerabilities research. Ego is longer important, and getting \$ for research on a free will basis is a proven capitalistic approach. What these companies(and I bet many more vendors will open themselves for

such a service) didn't take into consideration in my opinion, is that, starting to work with people giving \$ as the

ultimate incentive will prove tricky in the long-term.

What will happen of the Swiss cheese of software(yet the one that dominates 95 % of the OS market today)

Microsoft starts bidding for security vulnerabilities in its products? Bankruptcy is not an option, while I doubt they

will ever take this into consideration, mainly because it would seriously damage a market sector, the information

security one. Imagine, just for a sec. that Microsoft decides to seriously deal with all its vulnerabilities? But today's lack of accountability for software vendors' actions related to vulnerabilities is making it even worse. If MS doesn't

get sued for not releasing a patch in any time frame given, why should we, the small compared to MS vendor care?



Howard Schmidt, former White House cybersecurity adviser, once proposed that programmers should be held

responsible for releasing vulnerable code. I partly agree with him, you cannot cut costs in order to meet

product/marketing deadlines while hiring low skilled programmers who do not take security into consideration,

which opens another complex discussion on what should a developer focus on these days - efficiency or security,

and where's the trade-off?

7

I originally commented on this event back then :

*The position of Schmidt prompts him to address critical issues and look for very strategic solutions which may not be favored by the majority of the industry as I'm reading through various news comments and blogs. I personally think,*

*he has managed to realize the importance of making a distinction in how to tackle the vulnerabilities problem, who's*

*involved, and who can be influenced, where the ultimate goal is to achieve less vulnerable and poorly coded*

*software. Software vendors seek profitability, or might actually be in the survival stage of their existence, and as obvious as it may seem, they face huge costs, and extremely capable coders or employees tend to know their price!*

*What's the mention are the tech industry's "supposed to be" benchmarks for vulnerabilities management, picture an*

*enterprise with the "IE is the swiss cheese in the software world in terms of vulnerabilities, and yet no one is suing Microsoft over delayed patches" - lack of any incentives, besides moral ones, in case there're clear signs and*

*knowledge that efficiency is not balanced with security. And that's still a bit of a gray area in the development world.*

*Vulnerabilities simply cannot exist, and perhaps the biggest trade-off we should also face is the enormous growth of interactive applications, innovation approaches for disseminating information, with speeds far outpacing the level of attention security gets. Eventually, we all benefit out of it, web application vulnerabilities scanners and consultants get rich, perhaps the (ISC)<sup>2</sup> should take this into consideration as well :-)*

*Even though you could still do the following :*

- build awareness towards common certifications addressing the issue*
- ensure your coders understand the trade-offs between efficiency and security and are able to apply certain marginal thinking, whereas still meet their objectives*
- as far as accountability is concerned, do code auditing with security in mind and try figure out who are those that really don't have a clue about security, train them*
- constantly work on improving your patch release practices, or fight the problem from another point of view*

*But unless, coders, and software vendors aren't given incentives, or obliged under regulations (that would ultimately result in lack of innovation, or at least a definite slow down), you would again have to live with uncertainty, and*

*outsource the threats posed by this issue. Microsoft's "[12]Improving Web Application Security: Threats and Countermeasures" book, still provides a very relevant information.*

*[13]Slashdot's discussion*

What also bothers me, is how is the virginity of the vulnerability identified? I mean, what if I have already found it,

developed an exploit for it, sold it to the underground, and cashed with the industry as well, and no one came across

it on his/her :) honeyfarm? The researcher's reputation is a benchmark, but in the long-term, the competitive

market that's about to appear, will force the buyers to start working on a mass basis. There's a definitely a lot to

happen!

Welcome to the wonderful world of purchasing [14]0-day security vulnerabilities! Have an enemy, bid for his

ownage, have a competitor, own them without having to attract unnecessary attention, I'm just kiddin' of course,

although the possibilities are disturbing.

What I really liked about this important moment in vulnerability research, was that it was about time the security

researchers wanted to see how valued their research is in terms of the only currency that matters in the process -

the hard one. In my point of view, monetizing the vulnerabilities research market wasn't the best strategic approach

on fighting 0-day vulnerabilities, in this case, ensure you have the most impressive minds on your side, and that your

clients get hold of the latest vulnerabilities before the public does.

8

So - who's the winner - it's...[15]Symantec who first realized the long-term importance of security vulnerabilities, and where, both researchers and actual vulnerabilities are - Bugtraq/SecurityFocus, by [16]acquiring it for US \$75

million in cash, back in 2002, and later one integrating its joys into the [17]DeepSight Analyzer - remarkable. Both

from a strategic point of view, and mainly because that, by the time **any** post on **any** of the associated mailing lists doesn't get approved, it's Symantec's staff having first look at what's to come for the day of everyone.

SecurityFocus is running a story about the [18]Ebay vulnerability listing, and so is [19]eWeek, [20]Slashdot also

picked up the story. It was about time for everyone, given it actually happened during the weekend :-)

**UPDATE :** "[21]Where's my 0day, please?

Recommended reading can be found at :

[22]Vulnerability Disclosure Framework

[23]A Structured Approach to Classifying Security Vulnerabilities

[24]Guidelines for Security Vulnerability Reporting and Response

[25]Economic Analysis of Incentives to Disclose Software Vulnerabilities

[26]Impact of Software Vulnerability Announcements on the Market Value of Software Vendors – an Empirical

Investigation

[27]An Economic Analysis of Market for Software Vulnerabilities

[28]Market for Software Vulnerabilities? Think Again

[29]Talking about 0-day

Some stats :

[30]National Vulnerability Database

[31]CERT/CC Statistics 1988-2005

Technorati tags :

[32]security vulnerabilities,[33]vulnerabilities,[34]exploits ,  
[35]botnets,[36]0day,[37]full disclosure

1. [http://www.astalavista.com/media/archive1/newsletter/issue\\_19\\_2005.pdf](http://www.astalavista.com/media/archive1/newsletter/issue_19_2005.pdf)
2. <http://www.astalavista.com/index.php?section=newsletter>
3. <http://www.securityfocus.com/bid/15780/info>
4. <http://tippingpoint.com/>
5. <http://www.astalavista.com/index.php?section=directory&linkid=5703>
6. <http://photos1.blogger.com/blogger/1933/1779/1600/iDefense.gif>
7. <http://www.odefense.com/>
8. <http://www.zerodayinitiative.com/>
9. <http://photos1.blogger.com/blogger/1933/1779/1600/zero-day-initiative.jpg>
10. <http://www.odefense.com/>
11. <http://www.metasploit.com/>
12. <http://www.microsoft.com/downloads/details.aspx?FamilyId=E9C4BFAA-AF88-4AA5-88D4-0DEA898C31B9&displaylang=en>
13. <https://web.archive.org/web/20101016193540/http://it.slashdot.org/article.pl?sid=05/10/21/135204&tid=172&t>

[id=156](#)

14. <http://en.wikipedia.org/wiki/0-day>

15. <http://www.symantec.com/>

9

16. <http://www.symantec.com/press/2002/n020806.html>

17. <http://analyzer.securityfocus.com/>

18. <http://www.securityfocus.com/news/11363>

19. <http://www.eweek.com/article2/0,1895,1899697,00.asp>

20. <http://it.slashdot.org/it/05/12/12/1215220.shtml?tid=128&amp;amp;amp;amp;amp;amp;amp;tid=109&tid=>

[172&tid=98&tid=95&tid=8](#)

21. <http://ddanchev.blogspot.com/2006/03/wheres-my-0day-please.html>

22.  
<http://www.dhs.gov/interweb/assetlibrary/vdwgreport.pdf>

23.  
<http://www.sei.cmu.edu/pub/documents/05.reports/pdf/05tn003.pdf>

24.  
[http://www.oisafety.org/guidelines/Guidelines%20for%20Security%20Vulnerability%20Reporting%20and%20Resonse%20V2.0.pdf](http://www.oisafety.org/guidelines/Guidelines%20for%20Security%20Vulnerability%20Reporting%20and%20Response%20V2.0.pdf)

25. <http://infosecon.net/workshop/pdf/20.pdf>
26. [http://infosecon.net/workshop/pdf/telang\\_wattal.pdf](http://infosecon.net/workshop/pdf/telang_wattal.pdf)
27. <http://www.dtc.umn.edu/weis2004/kannan-telang.pdf>
28. [http://mansci.pubs.informs.org/e\\_companion\\_pages/May\\_05\\_EC/Kanan\\_Telang\\_EC.pdf](http://mansci.pubs.informs.org/e_companion_pages/May_05_EC/Kanan_Telang_EC.pdf)
29. [http://xcon.xfocus.org/archives/2005/Xcon2005\\_Sowhat.pdf](http://xcon.xfocus.org/archives/2005/Xcon2005_Sowhat.pdf)
30. <http://nvd.nist.gov/>
31. [http://www.cert.org/stats/cert\\_stats.html](http://www.cert.org/stats/cert_stats.html)
32. <http://technorati.com/tag/security+vulnerabilities>
33. <http://technorati.com/tag/vulnerabilities>
34. <http://technorati.com/tag/exploits>
35. <http://technorati.com/tag/botnets>
36. <http://technorati.com/tag/0day>
37. <http://technorati.com/tag/full+disclosure>

10

x

## **IP cloaking and competitive intelligence/disinformation (2005-12-14 16:36)**

[1]SearchSecurity.com are running a great article entitled "[2]IP cloaking becoming a business necessity", that I simply can't resist to express my opinion on.



[3]

Great concept that's been around since the days of  
[4]Anonymizer, who were perhaps the first enterprise to

start targeting enterprise and government

users looking for ways to hide their online activities, be it  
[5]unstructured data aggregation, [6]competitive

intelligence or simple end users' browsing.

Getting back to SearchSecurity's article, I don't really  
consider a company's SEC filings or annual reports (found  
on

any corporate web site) a trade secret! In this particular  
case, I bet it was extraordinary traffic from known partners  
that tipped them that there's a sudden interest in the  
company's business performance. Any organization could

easily look for patterns on its web server, such as how often  
certain stakeholders visit it, given they use their

associated netblocks, or ones known to be used by them.  
What to also note is that, given the stakeholders in this

case, employees, stockholders, suppliers, government, the  
general public or anyone else has a claim on the way the

organization operates, it would be hard, pretty much  
impossible to differentiate intentions of any of these.

Small companies can easily measure their popularity among  
the big players, again, given these companies use their

netblocks, but a large corporation with hundreds of  
thousands visitors, would have to put extra efforts in

measuring,

not only what's popular, but who's reading it, and are they on our watchlist.

How to compile these? Even though I'm certain someone out there has taken the time and effort to compile a

[7]Fortune 500 IP ranges list the way  
[8]GovernmentSecurity.org have compiled a [9]Government &Military; IP

ranges list. I soon expect to see companies offering segmented service for watchlists like the ones I mentioned, for

instance - law firms, financial institutions, non-profit organizations segmented on geographical location, let's say

New York or Tokyo based ones. An in-house approach can always be applied by any company, no matter of its size,

all you have to do is your homework at [10]RIPE.net for instance :

[11]RSA Security

[12]Symantec

[13]Sophos

[14]Kaspersky

[15]ISS(Internet Security Systems)

An important trend though, is how the transparency that the [16]ICANN wants to build whenever a domain is

registered in order to easily prosecute cyber criminals will open up countless opportunities for open source

intelligence professionals or wannabe's. A recently released [17]report by the [18]U.S Government Accountability

Office, found [19]2.3M domain names registered with false data, given that's just the result they came up by

sampling. Here're also the [20]important findings. Without any doubt, it should be known who's who in the

Internet's domain and IP blocks space, but knowing it and complying with this due to regulations, or good will is

going to lead to further consequences for your organization.

Let's take anti-virus vendors for instance. I often say that anti virus is a necessary evil - given it's active!! Signatures based defense is futile, windows of opportunities emerge faster, 0day threats contribute, and overall, malware is

starting to attack on a segmented based level => less major outbreaks, but the rates of signature updates is still a

benchmark the public and some of the vendors like talking about. [21]Email-Worm.Win32.Doombot.b for instance,

is a good example of how the malware author is rendering the antivirus software into a useless application, just by

blocking it from accessing its(publicly available, easy to find out through sniffin' etc.) update locations.

11

Even though the author wish he/she could "write" to these locations, that's not necessary, but the temporary

advantage of exposing the user/organization to a particular window of opportunity, by making sure access to

removal instructions and actual updates is disabled!

Doombot's list is short, and a bit of a common sense one

compared to [22]others. And as always, the general public, sick of ads, and parasites, have taken the effort to

constantly release updated [23]hosts files to tackle their concerns. I wonder when, and how are vendors going to

address this important from my point of view issue?

IP cloaking at the corporate level is still in its early stages, but represents a growing market due the following factors, among many others of course :

- governments and intelligence agencies are actively taking advantage of [24]open source intelligence, [25]OSINT,

and vendors are already starting to offer [26]relevant services. The Anonymizer among others, has also specially

government/enterprise tailored [27]services

- enterprises are getting extremely conscious about what others know of their surfing interests, and what are

stakeholders on their watchlist looking at, on any of their extranets or corporate web sites

- citizens from countries with extremely restrictive Internet censorship practices will fuel the market's growth even

more

Further reading can be found at :

[28]Protecting Corporations from Internet Counter-Intelligence

[29]Cloaking types

Technorati tags :

[30]competitive intelligence,[31]anonymity,[32]ip cloaking,  
[33]OSINT

1. <http://searchsecurity.techtarget.com/>
2. [http://searchsecurity.techtarget.com/originalContent/0,289142,sid14\\_gci1151253,00.html?track=sy160](http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1151253,00.html?track=sy160)
3. <http://photos1.blogger.com/blogger/1933/1779/1600/Anonymizer.gif>
4. <http://www.anonymizer.com/enterprise/solutions/>
5. <http://www.knowledgesearch.org/lsi/>
6. <https://web.archive.org/web/20101016193540/http://www.combsinc.com/handbook.htm>
7. <http://www.fortune.com/fortune/fortune500>
8. <http://www.governmentsecurity.org/>
9. <http://www.governmentsecurity.org/archive/t5818.html>
10. <http://www.ripe.net/>
11. <http://www.ripe.net/cgi-bin/search/gdquery.cgi?index=ripedb&amp;amp;amp;amp;amp;amp;file->

[match=ne](#)

[t%5B6n%5D&boolean=and&max-results=100&page-results=10&s](#)

12. <http://www.ripe.net/cgi-bin/search/gdquery.cgi?index=ripedb&file-match=ne>

[t%5B6n%5D&boolean=and&max-results=100&page-results=10&s](#)

13. <http://www.ripe.net/cgi-bin/search/gdquery.cgi?index=ripedb&file-match=ne>

[t%5B6n%5D&boolean=and&max-results=100&page-results=10&s](#)

14. <http://www.ripe.net/cgi-bin/search/gdquery.cgi?index=ripedb&file-match=ne>

[t%5B6n%5D&boolean=and&max-results=100&page-results=10&s](#)

15. <http://www.ripe.net/cgi-bin/search/gdquery.cgi?index=ripedb&file-match=net%5B>

[6n%5D&boolean=and&max-results=100&page-results=10&start](#)

16. <http://www.icann.org/>

17. <http://www.gao.gov/new.items/d06165.pdf>

18. <http://www.gao.gov/>

12

19. <http://www.networkworld.com/news/2005/120905-domain-names.html>

20. <http://www.gao.gov/highlights/d06165high.pdf>

21. <http://www.viruslist.com/en/viruses/encyclopedia?virusid=96944>

22. <http://www.viruslist.com/en/viruses/encyclopedia?virusid=74841>

23. <http://www.mvps.org/winhelp2002/hosts.txt>

24. [http://en.wikipedia.org/wiki/Open\\_source\\_intelligence](http://en.wikipedia.org/wiki/Open_source_intelligence)

25. <https://web.archive.org/web/20101016193540/http://www.cia.gov/csi/studies/vol48no3/article05.html>

26. <http://www.sail-technology.com/index.html?solutions/html/osint.html>

27. <http://www.anonymizer.com/government/solutions/>

28. [http://www.antiphishing.org/sponsors\\_technical\\_papers/Internet%20Counter-Intelligence%20White%20Paper.pdf](http://www.antiphishing.org/sponsors_technical_papers/Internet%20Counter-Intelligence%20White%20Paper.pdf)

29. [http://www.searchengineworld.com/misc/cloaking\\_agents.htm](http://www.searchengineworld.com/misc/cloaking_agents.htm)

30. <http://technorati.com/tag/competitive+intelligence>

31. <http://technorati.com/tag/anonymity>

32. <http://technorati.com/tag/ip+cloaking>

33. <http://technorati.com/tag/OSINT>

13

### **Insiders - insights, trends and possible solutions (2005-12-19 12:22)**

A recent research of the content monitoring market, and the U.S 2004's "[1]Annual Report to Congress on Foreign

Economic Collection and Industrial Espionage" I've recently read, prompted me to post an updated opinion on this

largely unsolved issue.

I have been keeping an eye on the insider problem for quite some time, in fact, I have featured a short article

entitled "**Insiders at the workplace - trends and practical risk mitigation approaches**" in [2]Issue 18 of the monthly

[3]security newsletter you can freely subscribe yourself to!

Insider as a definition can be as contradictive as the word "cheater" is :-) Does an individual become an insider even

when thinking about it, or turns into such prior to initiating an action defined as insider's one? The same way, can

someone be defined as a "cheater" just for thinking about what's perceived as cheating, compared to actually doing

anything?! :-) When does one become the other, and is this moment of any importance to tackling the problem?



The biggest trade-off as far as the insider's problem is concerned is between dealing with the problem while

ensuring productivity, and that the company's work environment isn't damaged – exactly the opposite. And while

productivity is extremely important, the direct, or most often indirect and long-term loss of intellectual property

theft is currently resulting in a couple of billion dollar unmaterialized revenues for nations/enterprises across the globe.

Going through 2004's “[4]Annual Report to Congress on Foreign Economic Collection and Industrial Espionage”, a

major trend needs to be highlighted as I greatly believe it's a global one, namely, private enterprises efforts to obtain access to sensitive technologies in unethical way, outpaces a foreign government's efforts to do the same.

Corporations spy more on one another than governments do, but is this truly accurate? I don't think so! The use of

freelancers, among them ex-intelligence officers or experienced detective agencies to conduct national funded

economic espionage is a growing trend, and the lines in this area are so blur, we should therefore try to grasp the big

picture when it comes to national competitiveness – both companies and nations directly/indirectly benefit from

possible economic/industrial espionage, and you can't deny it!

Yet another important fact to keep in mind, is the unusually high success of the oldest, and most common sense

social engineering attack – asking!! In certain cases a social engineer will inevitably establish contact with

customer-service obsessed personnel taking care of you all your requests! A certain organization's members may

experience troubles differentiating sensitive and secret information, not taking the first one as serious as they

should. Even worse – U.S Secret Service and CERT's “[5]Insider threat Study : Illicit Cyber Activity in the Banking and

Finance sector” reveal that,” *83 % of the insider threat cases took place physically from within the insider's*

*organization, and another 70 % in all cases, the incidents took place during normal working hours”!* No secretaries or CEO's logging in at 3:00AM, and in this case, the lack of detected security incidents posed by insiders, means they

are already happening!

Though, I have always looked at the insider's issue, from both negative and positive point of view. Can an insider be

of any use for the good of a free speech organization or a government? Yes, it can if you take into account the U.S

government's efforts to locate democratically minded individuals living in countries with restrictive regimes, or

active Internet censorship efforts.

Now given, you are truly interested in the democratization of this particular region, and not another successful

[6]PSYOPS operation, being able to locate, establish, and actually, maintain contact with these individuals will prove

crucial in case of a objective picture of what exactly is going on there! Ignoring the local, totally biased news

streaming for certain regions, and focusing on locating insiders within rogue states has been a common practice for years.

14

Is there a market for protecting from intellectual property theft and sensitive information leakage? If so, how does it ensures today's digital workplace, and road warriors's flexibility is not sacrificed for the sake of protecting the

company's resources? Mind you, the current solutions scratch only the surface of the issue - creating digital

signatures of data and trying to spot it leaving the network. While a commonly accepted approach, it's like one way

authentication(passwords) when it comes to access control- the first line of defense, but among the many other!

The insiders' problem is far more broader one and given the today's complexity and connectivity, a possible insider's

actions will most often constitute of normal daily activities. But what is the market up to anyway?

Currently, the content monitoring market is steadily growing fueled by the need of ensuring information marked as

sensitive, or intellectual property doesn't leave the company's premises, or is alerted when someone attempts to

transfer it, due to negligence or on purposely!

The main players are : [7]Vontu, [8]Tablus, [9]Reconnex, and [10]Vericept.

Whereas these solutions are a great [11]concept, they all mainly rely on content analysis, and sensitive information

signatures, monitoring multiple exit point)[12] (email, web, chats, forums, p2p, ftp, even telnet), namely, reactive

protection, while sophisticated insider's actions may remain hidden due to covert channels or 0day vulnerabilities in

the vendor's product for instance!

[13][14][15]Something else to consider, is should a IP(intellectual property) trap be considered as a benchmark for

insider tensions?! In other words, should you consider an employee that has been on purposely sent a link

containing company information he/she isn't supposed to have access to, but has clicked to obtain it? [16]Stanford

[17][18]thinks - yes! The University suspended potential candidates for obtaining info on their admission process

only by following a link..you are either a one or zero, right?

[19][20]Honeypots targeting insiders have [21]also been discussed a long time ago by [22]Lance Spitzner, from the

Honeynet Project. Another proactive protection would be to look for patterns defined as malicious behavioral based mostly.

**From an organization's point of view, take into consideration the following :**

- Clearly communicate the consequences, both individual and career, in case an insider is somehow identified, based on the company's perception of the problem

- Ensure the momentum of negative attitude towards the organization is minimized to the minimum to ensure the lack of to-be-developed post-effect negative sentiments

- Do not fall victim of the common misunderstanding that technology is the key to the solution. Insiders are the people your technology resources empower to do their daily tasks, technology is as often happens, the facilitator of certain actions

- Does system identification accountability have any actual effect? My point, does a user's loss of accounting data, resulting in successful attack is anyhow prosecuted/tolerated. If it isn't, this puts any employee in extremely

favorable "it wasn't my fault" position, where the data could be shared, on purposely exposed, sold, pretended to be stolen etc.

- Building active awareness towards the company's efforts and commitment to fighting the problem will inevitably

discourage the less motivated wannabe insiders, or at least make them try harder!

**From a nation's point of view, the following issues should be taken into consideration :**

15

- In today's increasingly transparent and based on digital flow of information marketplace, open source intelligence capabilities played a leading role in the development of cost-effective competitive intelligence solutions. Even

though, nations or their companies are very interested in exploiting today's globalized world.

- Ensuring the adequate security level of the private and academic sectors' infrastructure (where research turns into products and services, or exactly the opposite) through legislations, or further incentives, will improve the national competitiveness, while preserving the current R & D innovations, as secret as necessary.

- Outsourcing should be considered as a important factor contributing to information leakage, and the individuals involved, or the company's screening practices, should be carefully examined.

- A fascinating publication that I recently read is "[23]Quantifying National Information Leakage" describing the

implications of the Internet's distributed nature, namely to what extent, U.S Internet traffick is leaking around the world, where it "passes by". A nation's habit or lack of efficient alternative of plain-text communications can prove tricky if successfully exploited. Of course, this doesn't include conspiracy scenarios of major certificate authorities breached into.

The insiders' problem will remain an active topic for discussion for years to come given its complexity and severity of

implications. Insiders's metrics are a key indicator for patterns tracking, whereas their creativity shouldn't be underestimated at any cost!

In case you are interested in various recommended reading, statistics, and other people's point of view, try this

research :

[24]Understanding the Insider Threat - Proceedings of a March, 2004 Workshop

[25]A Target-Centric Formal Model For Insider Threat and More

[26]Analysis and Detection of Malicious Insiders

[27]Insider Threat : Real Data on a Real Problem

[28]Insider Threat Study : Computer System Sabotage in Critical Infrastructure Sectors

[29]Preliminary System Dynamics Maps of the Insider Cyber-threat Problem

[30]Technological, Social, and Economic Trends That Are Increasing U.S. Vulnerability to Insider Espionage

[31]Preventing Insider Sabotage : Lessons Learned From Actual Attacks

Technorati tags : [32]insiders,[33]insider,[34]espionage,[35]enterprise risk

management,[36]security,[37]information security

1.

[http://www.nacic.gov/publications/reports\\_speeches/reports/fecie\\_all/fecie\\_2004/FecieAnnual%20report\\_2004\\_N](http://www.nacic.gov/publications/reports_speeches/reports/fecie_all/fecie_2004/FecieAnnual%20report_2004_N)

[oCoverPages.pdf](#)

2.

[http://www.astalavista.com/media/archive1/newsletter/issue\\_18\\_2005.pdf](http://www.astalavista.com/media/archive1/newsletter/issue_18_2005.pdf)

3. <http://www.astalavista.com/index.php?section=newsletter>

4.

[http://www.nacic.gov/publications/reports\\_speeches/reports/fecie\\_all/fecie\\_2004/FecieAnnual%20report\\_2004\\_N](http://www.nacic.gov/publications/reports_speeches/reports/fecie_all/fecie_2004/FecieAnnual%20report_2004_N)

[oCoverPages.pdf](#)

5. <http://www.cert.org/archive/pdf/bankfin040820.pdf>

6. <http://en.wikipedia.org/wiki/Psyops>

7. <http://www.vontu.com/>



8. <http://www.tablus.com/>
9. <http://www.reconnex.net/>
10. <http://www.vericept.com/>
- 16
11.  
[http://photos1.blogger.com/blogger/1933/1779/1600/vericept\\_logo.gif](http://photos1.blogger.com/blogger/1933/1779/1600/vericept_logo.gif)
12. <http://vontu.com/images/global/vontu.gif>
13.  
<http://photos1.blogger.com/blogger/1933/1779/1600/tablus.gif>
14. [http://images.tablus.com/new\\_home/logo2.gif](http://images.tablus.com/new_home/logo2.gif)
15.  
<http://photos1.blogger.com/blogger/1933/1779/1600/logo2.gif>
16.  
<http://www.computerworld.com/printthis/2005/0,4814,100206,00.html>
17. [http://www.reconnex.net/images/nav/recon\\_logo.gif](http://www.reconnex.net/images/nav/recon_logo.gif)
18.  
<http://www.computerworld.com/printthis/2005/0,4814,100206,00.html>
19.  
[http://photos1.blogger.com/blogger/1933/1779/1600/vericept\\_logo.1.gif](http://photos1.blogger.com/blogger/1933/1779/1600/vericept_logo.1.gif)

20. <http://winfingerprint.sourceforge.net/presentations/honeyne-t-insider-threat-2004.ppt>
21. [http://www.vericept.com/00\\_images/shared\\_images/vericept\\_logo.gif](http://www.vericept.com/00_images/shared_images/vericept_logo.gif)
22. <http://www.spitzner.net/>
23. [http://www.cs.cmu.edu/~dwendlan/info\\_leak.pdf](http://www.cs.cmu.edu/~dwendlan/info_leak.pdf)
24. [http://rand.org/pubs/conf\\_proceedings/2005/RAND\\_CF196.pdf](http://rand.org/pubs/conf_proceedings/2005/RAND_CF196.pdf)
25. <http://www.cse.buffalo.edu/tech-reports/2004-16.pdf>
26. [https://analysis.mitre.org/proceedings/Final\\_Papers\\_Files/280\\_Camera\\_Ready\\_Paper.pdf](https://analysis.mitre.org/proceedings/Final_Papers_Files/280_Camera_Ready_Paper.pdf)
27. <http://www.cert.org/archive/pdf/CSI-Presentation.pdf>
28. [http://www.secretservice.gov/ntac/its\\_report\\_050516\\_es.pdf](http://www.secretservice.gov/ntac/its_report_050516_es.pdf)
29. <http://www.cert.org/archive/pdf/InsiderThreatSystemDynamics.pdf>
30. <http://www.fas.org/sgp/othergov/dod/insider.pdf>
31. <http://www.cert.org/archive/pdf/InsiderThreatCSI.pdf>
32. <http://technorati.com/tag/insiders>
33. <http://technorati.com/tag/insider>

- 34. <http://technorati.com/tag/espionage>
- 35. <http://technorati.com/tag/enterprise+risk+management>
- 36. <http://technorati.com/tag/security>
- 37. <http://technorati.com/tag/information+security>

17

### **Cyberterrorism - don't stereotype and it's there! (2005-12-19 15:27)**

I wrote my first article on "[1]Cyberterrorism – an analysis"(in Bulgarian, [2]HiComm Magazine) back in 2003,

arguing that Cyberterrorism is a fully realistic scenario, given you don't picture terrorists melting down nuclear

power plants over the Internet, but an organization determined to achieve all of its objectives, and using the digital

medium to do so.

My second article "[3]Cyberterrorism and Cyberwars - how real's the threat?"(in Bulgarian, [4]CIO.bg) was greatly extended, and so was my understanding of the concept by the time. I often come across badly structured articles on

the topic, even worse, ones starting to discuss the wrong concept – the biased one! Where terrorists try to attack

the critical infrastructure, well, they wouldn't, they'd rather abuse instead of destroying it!

Merely evaluating a terrorist groups ability to conduct devastating DDoS attacks, or hack into U.S government

computers, is the biased wrong concept I just mentioned. If terrorist groups want DDoS power, they wouldn't

rewrite their training manuals, instead, they would simply hire the people to do it, or request on point'n'click

interface for their actions. Can this kill a person? If yes, how come, if not, is this Cyberterrorism at all?

Thinking about complex topics always involves dimensional approach, understanding of motives, and implying a

little bit of marginal thinking to grasp the big picture. Terrorists killing people over the Internet myth is greatly

influenced by the success of any terrorist organization's "PR" activities – spread fear, and build active propaganda

though taking lives, and distributing the freely available media later on. So, if no lives are taken, why call it

terrorism? Mainly because, cyberterrorism in my point of view isn't an entirely new concept as some try to put it,

it's an extension of real life terrorism activities into cyberspace, and its evolution at a later stage.

Starting from the basic premises that terrorists need to communicate with each other, keep themselves up-to-date

in today's [5]OSINT(open-source intelligence world), recruit potential members, and continue their active

propaganda taking advantage of Internet's many joys, in respect to anonymity(given it's achieved), speed, and a bit

of a black humor – interactivity!

Cyberterrorism as a concept from my point of view consists of their need for :

**- platform for communication**

No other medium can provide better speed, connectivity, and most importantly anonymity, given it's achieved and

understood, and it often is. Plain encryption might seem the obvious answer, but to me it's [6]steganography, having

the potential to fully hide within legitimate (at least looking) data flow. Another possibility is the use secret sharing schemes. A bit of a relevant tool that can be fully utilized by any group of people wanting to ensure their

authenticity and perhaps everyone's pulse, is [7]SSSS - Shamir's Secret Sharing Scheme. And no, I'm not giving tips,

just shredding light on the potential in here! The way botnets of malware can use public forums to get commands,

in this very same fashion, terrorists could easily hide sensitive communications by mixing it with huge amounts of public data, while still keeping it secret.

**- platform for open source intelligence**

Undoubtedly, there has never been so much publicly accessible information that could aid in the organizing and

plotting terrorist acts. Measure the impact of a certain bombing? - check out the news and figure out what has

changed ever since, research and obtain digital photos, even satellite imagery, it's available. Try to figure out the latest specifications for RFID passports to come, and why it matters to you – keep on reading the specifications..!

Transparency is always tricky!

The way a government can successfully identify terrorist sentiments around the Web, even precise sites to be put

under close surveillance, terrorists on the other hand keep track of each and every major/minor global change

anyhow affecting their goals or ambitions.

### **- platform for propaganda/recruitment**

Now, don't picture "Outstanding CV, here's the address of our training camp in Pakistan, please, first introduce the

idea to your friends, then share the address. Nuke the planet!" type of conversation :-)

Recruitment over the Internet is a contradictory topic, and many will argue that it's irrelevant. I can argue too that

there are people for all kinds of things, from maintaining mailings lists, to acting as freelancers whenever a resource, like an infected PC for anonymous communication is needed. Believe it or not, terrorists are silently but very actively

building a web presence. In fact, these days you could even download execution clips directly from a terrorist's web

site. What's else to note is the irony of how many [8]terrorists web sites are actually hosted on U.S service

provider's servers, and you keep on looking for them around the world, check your backyard before looking at the neighbors :-)

Another important aspect of recruiting in such a way, is the location of people with obsessive

islamic views, someone actively expressing his/her hate towards the U.S and actually being of any use. For instance,

there are cases of terrorist propaganda malware, where the author(a teenager, or sophisticated attacks?!) clearly

expresses his/her support towards a "cause".

This case is like the one I mentioned in my previous post concerning [9]insiders, that is the way U.S government

looks for [10]democracy minded individuals in restrictive regime countries(the Win32/Cycle.A.worm), the very same

way terrorists could spot similarly minded individuals holding important positions or knowledge on certain topic.

Are any of these people screaming for recruitment, and would somebody listen?

**- direct attack exploitation possibilities (people eventually die?!)**

Is the electronically obtained a major food manufacturer's facility truck schedules of any use to terrorists interested

in eventually hijacking and

Someone once mentioned a scenario related to [11]U.S RFID passports, namely a bomb could automatically

detonate, given there're certain number of "broadcasted", note the term, U.S citizens around, that's scary, but how about the same applies to mobile malware detecting U.S carriers for the same purpose?!

In the last [12]article I wrote on the topic, I made an argument on where's the line of a 19 year's old boy shutting down 911 through ingenious technique for the fun of it, and a terrorist organization exploiting vulnerability in the system at a crucial moment in time let's say?! What if people die out of the teen's actions, but the terrorists' attempt is quickly detected? Should cyberterrorism be judged based on the motives, or who's actually behind it? I think it's a combination of both!

### **- indirect attack exploitation possibilities**

Should a terrorists' use of phishing attacks, where the revenues go directly into funding further terrorist activities, both, cyber, real-life actions be considered an option?

Should a terrorist's actions for hiring a person, directly obtaining certain social numbers, sensitive and detailed financial information, or anything else to assist a successful identity theft, with the idea to impersonate for a real-life terrorist scenario be considered an option? Yes, they both should!

19

This particular list is endless, the scenarios I can only leave to someone else's psychological



imagination!

My worst case scenarios, though, consist of terrorists realizing the impact a target/mass directed intellectual

property theft, [13]cryptoviral extortion attack targeting the majority of U.S businesses. And as I often say, it's all a matter of coordination with the idea to increase the impact!

To conclude, *Terrorists are not rocket scientists unless we make them feel so!*

Consider going through the following research for different point of views, and key facts :

[14]How Modern Terrorism Uses the Internet

[15]Examining the Cyber Capabilities of Islamic Terrorist Groups

[16]The Power Failure and the Internet

[17]Telecom - The Terrorism Risk

[18]Emerging Terrorist Capabilities for Cyber Conflict against the U.S. Homeland

[19]Myths and Realities of Cyberterrorism

[20]Terrorism, Cyberspace and The First Amendment

[21]Information Warfare: The Perfect Terrorist Weapon

[22]Cyberland Security: Organised Crime, Terrorism and The Internet

[23]Cyber Terrorism: Mass Destruction or Mass Disruption?

[24]Cyber Warfare: An Analysis of the Means and Motivations of Selected Nation States

Technorati tags : [25]cyberterrorism, [26]terrorism, [27]al qaeda, [28]internet terrorism

1. <http://www.frame4.com/content/hicomm/mar-2003-hicomm.pdf>
2. <http://www.hicomm.bg/>
3. <http://www.astalavista.com/index.php?section=directory&linkid=4954>
4. <http://www.cio.bg/>
5. <http://en.wikipedia.org/wiki/OSINT>
6. <http://en.wikipedia.org/wiki/Steganography>
7. <http://point-at-infinity.org/ssss/>
8. <http://haganah.org.il/hmedia/08feb05-WND-06feb05-hizballah.pdf>
9. <http://ddanchev.blogspot.com/2005/12/insiders-insights-trends-and-possible.html>
10. <http://www.ravantivirus.com/virus/showvirus.php?v=216>
11. <http://edocket.access.gpo.gov/2005/05-21284.htm>
12. <http://www.astalavista.com/index.php?section=directory&linkid=4954>
13. <http://www.cryptovirology.com/cryptovfiles/cryptovirologyfaqver1.html>

14. <http://www.usip.org/pubs/specialreports/sr116.pdf>
15. <http://www.ists.dartmouth.edu/library/164.pdf>
16. <http://www.ists.dartmouth.edu/library/120.pdf>
17. <http://www.pvtr.org/pdf/1%20CFT%20and%20Telecom%20article.pdf>
18. <http://www.cyberconflict.org/pdf/WilsonPresentation.pdf>
19. <http://www.comm.ucsb.edu/Research/Myths%20and%20Realities%20of%20Cyberterrorism.pdf>
20. [http://www.lawtechjournal.com/articles/2004/04\\_041207\\_margulies.pdf](http://www.lawtechjournal.com/articles/2004/04_041207_margulies.pdf)
- 20
21. <http://www.ict.org.il/articles/infowar.htm>
22. [http://www.oii.ox.ac.uk/collaboration/lectures/20050210\\_maitai\\_speech\\_v1.0\\_web.pdf](http://www.oii.ox.ac.uk/collaboration/lectures/20050210_maitai_speech_v1.0_web.pdf)
23. <http://www.crime-research.org/library/mi2g.htm>
24. <http://www.ists.dartmouth.edu/directors-office/cyberwarfare.pdf>
25. <http://technorati.com/tag/cyberterrorism>
26. <http://technorati.com/tag/terrorism>
27. <http://technorati.com/tag/al+qaeda>

28. <http://technorati.com/tag/internet+terrorism>

21

### **Insiders - insights, trends and possible solutions (2005-12-19 15:33)**

A recent research of the content monitoring market, and the U.S 2004's "[1]Annual Report to Congress on Foreign

Economic Collection and Industrial Espionage" I've recently read, prompted me to post an updated opinion on this

largely unsolved issue.

I have been keeping an eye on the insider problem for quite some time, in fact, I have featured a short article

entitled "**Insiders at the workplace - trends and practical risk mitigation approaches**" in [2]Issue 18 of the monthly

[3]security newsletter you can freely subscribe yourself to!

Insider as a definition can be as contradictive as the word "cheater" is :-) Does an individual become an insider even

when thinking about it, or turns into such prior to initiating an action defined as insider's one? The same way, can

someone be defined as a "cheater" just for thinking about what's perceived as cheating, compared to actually doing

anything?! :-) When does one become the other, and is this moment of any importance to tackling the problem?

The biggest trade-off as far as the insider's problem is concerned is between dealing with the problem while

ensuring productivity, and that the company's work environment isn't damaged – exactly the opposite. And while

productivity is extremely important, the direct, or most often indirect and long-term loss of intellectual property

theft is currently resulting in a couple of billion dollar unmaterialized revenues for nations/enterprises across the globe.

Going through 2004's "[4]Annual Report to Congress on Foreign Economic Collection and Industrial Espionage", a

major trend needs to be highlighted as I greatly believe it's a global one, namely, private enterprises efforts to obtain access to sensitive technologies in unethical way, outpaces a foreign government's efforts to do the same.

Corporations spy more on one another than governments do, but is this truly accurate? I don't think so! The use of

freelancers, among them ex-intelligence officers or experienced detective agencies to conduct national funded

economic espionage is a growing trend, and the lines in this area are so blur, we should therefore try to grasp the big

picture when it comes to national competitiveness – both companies and nations directly/indirectly benefit from

possible economic/industrial espionage, and you can't deny it!

Yet another important fact to keep in mind, is the unusually high success of the oldest, and most common sense

social engineering attack – asking!! In certain cases a social engineer will inevitably establish contact with

customer-service obsessed personnel taking care of you all your requests! A certain organization's members may

experience troubles differentiating sensitive and secret information, not taking the first one as serious as they

should. Even worse – U.S Secret Service and CERT's “[5]Insider threat Study : Illicit Cyber Activity in the Banking and

Finance sector” reveal that,” *83 % of the insider threat cases took place physically from within the insider's*

*organization, and another 70 % in all cases, the incidents took place during normal working hours”!* No secretaries or CEO's logging in at 3:00AM, and in this case, the lack of detected security incidents posed by insiders, means they

are already happening!

Though, I have always looked at the insider's issue, from both negative and positive point of view. Can an insider be

of any use for the good of a free speech organization or a government? Yes, it can if you take into account the U.S

government's efforts to locate democratically minded individuals living in countries with restrictive regimes, or

active Internet censorship efforts.

Now given, you are truly interested in the democratization of this particular region, and not another successful

[6]PSYOPS operation, being able to locate, establish, and actually, maintain contact with these individuals will prove crucial in case of a objective picture of what exactly is going on there! Ignoring the local, totally biased news streaming for certain regions, and focusing on locating insiders within rogue states has been a common practice for years.

22

Is there a market for protecting from intellectual property theft and sensitive information leakage? If so, how does it ensures today's digital workplace, and road warriors's flexibility is not sacrificed for the sake of protecting the company's resources? Mind you, the current solutions scratch only the surface of the issue – creating digital signatures of data and trying to spot it leaving the network. While a commonly accepted approach, it's like one way authentication(passwords) when it comes to access control–the first line of defense, but among the many other!

The insiders' problem is far more broader one and given the today's complexity and connectivity, a possible insider's actions will most often constitute of normal daily activities. But what is the market up to anyway?

Currently, the content monitoring market is steadily growing fueled by the need of ensuring information marked as sensitive, or intellectual property doesn't leave the company's premises, or is alerted when someone attempts

to

transfer it, due to negligence or on purposely!

The main players are : [7]Vontu, [8]Tablus, [9]Reconnex, and [10]Vericept.

Whereas these solutions are a great concept, they all mainly rely on content analysis, and sensitive information

signatures, monitoring multiple exit point)  
(email, web, chats, forums, p2p, ftp, even telnet), namely,  
reactive

protection, while sophisticated insider's actions may remain hidden due to covert channels or 0day vulnerabilities in

the vendor's product for instance!

Something else to consider, is should a IP(intellectual property) trap be considered as a benchmark for insider

tensions?! In other words, should you consider an employee that has been on purposely sent a link containing

company information he/she isn't supposed to have access to, but has clicked to obtain it? [11]Stanford [12]thinks -

yes! The University suspended potential candidates for obtaining info on their admission process only by following a

link..you are either a one or zero, right?

[13]Honeypots targeting insiders have also been discussed a long time ago by [14]Lance Spitzner, from the Honeynet

Project. Another proactive protection would be to look for patterns defined as malicious behavioral based mostly.



**From an organization's point of view, take into consideration the following :**

- Clearly communicate the consequences, both individual and career, in case an insider is somehow identified, based on the company's perception of the problem

- Ensure the momentum of negative attitude towards the organization is minimized to the minimum to ensure the lack of to-be-developed post-effect negative sentiments

- Do not fall victim of the common misunderstanding that technology is the key to the solution. Insiders are the people your technology resources empower to do their daily tasks, technology is as often happens, the facilitator of certain actions

- Does system identification accountability have any actual effect? My point, does a user's loss of accounting data, resulting in successful attack is anyhow prosecuted/tolerated. If it isn't, this puts any employee in extremely

favorable "it wasn't my fault" position, where the data could be shared, on purposely exposed, sold, pretended to be stolen etc.

- Building active awareness towards the company's efforts and commitment to fighting the problem will inevitably

discourage the less motivated wannabe insiders, or at least make them try harder!

**From a nation's point of view, the following issues should be taken into consideration :**

- In today's increasingly transparent and based on digital flow of information marketplace, open source intelligence capabilities played a leading role in the development of cost-effective competitive intelligence solutions. Even though, nations or their companies are very interested in exploiting today's globalized world.

23

- Ensuring the adequate security level of the private and academic sectors' infrastructure (where research turns into products and services, or exactly the opposite) through legislations, or further incentives, will improve the national competitiveness, while preserving the current R & D innovations, as secret as necessary.

- Outsourcing should be considered as a important factor contributing to information leakage, and the individuals involved, or the company's screening practices, should be carefully examined.

- A fascinating publication that I recently read is "[15]Quantifying National Information Leakage" describing the

implications of the Internet's distributed nature, namely to what extent, U.S Internet traffick is leaking around the

world, where it "passes by". A nation's habit or lack of efficient alternative of plain-text communications can prove

tricky if successfully exploited. Of course, this doesn't include conspiracy scenarios of major certificate authorities breached into.

The insiders' problem will remain an active topic for discussion for years to come given its complexity and severity of

implications. Insiders's metrics are a key indicator for patterns tracking, whereas their creativity shouldn't be underestimated at any cost!

In case you are interested in various recommended reading, statistics, and other people's point of view, try this research :

[16]Understanding the Insider Threat - Proceedings of a March, 2004 Workshop

[17]A Target-Centric Formal Model For Insider Threat and More

[18]Analysis and Detection of Malicious Insiders

[19]Insider Threat : Real Data on a Real Problem

[20]Insider Threat Study : Computer System Sabotage in Critical Infrastructure Sectors

[21]Preliminary System Dynamics Maps of the Insider Cyber-threat Problem

[22]Technological, Social, and Economic Trends That Are Increasing U.S. Vulnerability to Insider Espionage

[23]Preventing Insider Sabotage : Lessons Learned From Actual Attacks

Technorati tags : [24]insiders,[25]insider,[26]espionage,[27]enterprise risk

management,[28]security,[29]information security

1.  
[http://www.nacic.gov/publications/reports\\_speeches/reports/fecie\\_all/fecie\\_2004/FecieAnnual%20report\\_2004\\_N](http://www.nacic.gov/publications/reports_speeches/reports/fecie_all/fecie_2004/FecieAnnual%20report_2004_N)

[oCoverPages.pdf](#)

2.  
[http://www.astalavista.com/media/archive1/newsletter/issue\\_18\\_2005.pdf](http://www.astalavista.com/media/archive1/newsletter/issue_18_2005.pdf)

3.  
<https://draft.blogger.com/http://www.astalavista.com/index.php?section=newsletter>

4.  
[http://www.nacic.gov/publications/reports\\_speeches/reports/fecie\\_all/fecie\\_2004/FecieAnnual%20report\\_2004\\_N](http://www.nacic.gov/publications/reports_speeches/reports/fecie_all/fecie_2004/FecieAnnual%20report_2004_N)

[oCoverPages.pdf](#)

5. <http://www.cert.org/archive/pdf/bankfin040820.pdf>

6. <http://en.wikipedia.org/wiki/Psyops>

7. <http://www.vontu.com/>

8. <http://www.tablus.com/>

9. <http://www.reconnex.net/>

10. <http://www.vericept.com/>

11.

[https://web.archive.org/web/20101016193540/http://www.computerworld.com/printthis/2005/0,4814,100206,00.](https://web.archive.org/web/20101016193540/http://www.computerworld.com/printthis/2005/0,4814,100206,00.html)

[html](#)

24

12.

<http://www.computerworld.com/printthis/2005/0,4814,100206,00.html>

13.

<http://winfingerprint.sourceforge.net/presentations/honeyne-t-insider-threat-2004.ppt>

14. <http://www.spitzner.net/>

15. [http://www.cs.cmu.edu/~dwendlan/info\\_leak.pdf](http://www.cs.cmu.edu/~dwendlan/info_leak.pdf)

16.

[http://rand.org/pubs/conf\\_proceedings/2005/RAND\\_CF196.p  
df](http://rand.org/pubs/conf_proceedings/2005/RAND_CF196.pdf)

17. <http://www.cse.buffalo.edu/tech-reports/2004-16.pdf>

18.

[https://analysis.mitre.org/proceedings/Final\\_Papers\\_Files/280\\_Camera\\_Ready\\_Paper.pdf](https://analysis.mitre.org/proceedings/Final_Papers_Files/280_Camera_Ready_Paper.pdf)

19. <http://www.cert.org/archive/pdf/CSI-Presentation.pdf>

20.

[http://www.secretservice.gov/ntac/its\\_report\\_050516\\_es.pdf](http://www.secretservice.gov/ntac/its_report_050516_es.pdf)

21. <http://www.cert.org/archive/pdf/InsiderThreatSystemDynamics.pdf>
22. <http://www.fas.org/sgp/othergov/dod/insider.pdf>
23. <http://www.cert.org/archive/pdf/InsiderThreatCSI.pdf>
24. <http://technorati.com/tag/insiders>
25. <http://technorati.com/tag/insider>
26. <http://technorati.com/tag/espionage>
27. <http://technorati.com/tag/enterprise+risk+management>
28. <http://technorati.com/tag/security>
29. <http://technorati.com/tag/information+security>

25

26

**2.**

**2006**

27

**2.1**

**January**

28

**What's the potential of the IM security market?  
Symantec thinks big (2006-01-04 12:18)**

Yesterday, Symantec, one of the world's leading security, and of course, storage providers [1]acquired [2]IMlogic, a leading provider of Instant Messaging security solutions. How sound is this move anyway? Doesn't Symantec already have the [3]necessary [4]experience in this field?

IMlogic has never been a build-to-ship company. Dating back to 2002, it has managed to secure important customers,

Fortune 1000 companies as a matter of fact, and acts as a preferred choice for many of them. And given that

enterprise IM is exploding, and so is home use, the real-time nature of this type of communication has always been

acting as a hit-list in my mind. Client based vulnerabilities, social engineering attacks, auto-responding malware, and many other issues are among the current trends.

How huge is the potential of IM security, or is it me just trying to think big in here, compared to Symantec's simple product line extension ambition? Besides acting as another propagation vector for future malware releases, IM

usage worldwide is already outpacing the most common form of Internet communication - the email. A Radicati

Group's research report entitled "[5]Instant Messaging and Presence Market Trends, 2003-2007" indicates the same.

The group [6]predicts that :

[7][8] - 1,439 million IM accounts in existence by 2007

- a very significant increase in corporate implementation of IM, from 60 million accounts today to 349 million in 2007.

- that's a degree of monopoly, as always!

Lucky you, Symantec!

With fear of being a pessimist, I have though witnessed how unique organizations and teams got eventually

swallowed by the corporate world. And it's [9]their know-how that I truly miss these days.

You can though, still go through Symantec's constantly updating list of [10]acquired companies, and it's evident they

are fully committed to continue being a market and knowledge leader. I also recommend you read a great article at

eWeek entitled [11]IM Threats : The Dark Side of Innovation to find out more about the current trends. What's your

attitude about them?!

Technorati tags :

[12]Symantec, [13]IM, [14]security, [15]information security

1. [http://www.symantec.com/about/news/release/article.jsp?prid=20060103\\_01](http://www.symantec.com/about/news/release/article.jsp?prid=20060103_01)

2. <http://www.imlogic.com/>

3. <http://securityresponse.symantec.com/avcenter/reference/secure.instant.messaging.pdf>



4.

<http://securityresponse.symantec.com/avcenter/reference/threats.to.instant.messaging.pdf>

5. [http://www.ostermanresearch.com/or\\_im05es.pdf](http://www.ostermanresearch.com/or_im05es.pdf)

29

6.

[http://online.wsj.com/public/article/SB112907349731466067-fB0n6k6c3HC\\_Kcim4M6p9jHeagE\\_20061011.html?mod=public\\_home\\_us](http://online.wsj.com/public/article/SB112907349731466067-fB0n6k6c3HC_Kcim4M6p9jHeagE_20061011.html?mod=public_home_us)

[public\\_home\\_us](http://online.wsj.com/public/article/SB112907349731466067-fB0n6k6c3HC_Kcim4M6p9jHeagE_20061011.html?mod=public_home_us)

7. [http://online.wsj.com/public/resources/images/MK-AF175\\_MSN\\_YA10112005182104.gif](http://online.wsj.com/public/resources/images/MK-AF175_MSN_YA10112005182104.gif)

8. [http://online.wsj.com/public/resources/images/MK-AF175\\_MSN\\_YA10112005182104.gif](http://online.wsj.com/public/resources/images/MK-AF175_MSN_YA10112005182104.gif)

9. <http://www.atstake.com/>

10.

<http://www.symantec.com/about/profile/development/acquisitions/index.jsp>

11. <http://www.eweek.com/article2/0,1895,1904984,00.asp>

12. <http://technorati.com/tag/Symantec>

13. <http://technorati.com/tag/IM>

14. <http://technorati.com/tag/security>

15. <http://technorati.com/tag/information+security>

30

## **Keep your friends close, your intelligence buddies closer! (2006-01-04 13:11)**

[1]Too much power always leads you to the dark side!

[2]Cryptome has yesterday [3]featured a excerpt from "[4]State of the War : The Secret History of the CIA and the

Bush Administration" shredding more light on what the NSA used to be before 9/11 and how things changed at a

later stage. In case you really want to find out more about the entire history of the NSA, go though "[5]The Quest for Cryptologic Centralization and the Establishment of NSA, 1940-1952", and some of the most remarkable NSA

released publication entitled "[6]Eavesdropping on Hell : Historical Guide to Western Communications Intelligence and the Holocaust, 1939-1945".

My opinion - With no guards, the gates are always open. But who will watch the watchers when they start watching us?!

Even though, as Marine Corps General Alfred M. Gray have put it years ago "Communications without intelligence is noise, intelligence without communications is irrelevant", and so is privacy in the 21st century, period.

Technorati tags :

[7]NSA, [8]intelligence, [9]eavesdropping, [10]CIA

1. <http://www.tlio.demon.co.uk/eyesky.jpg>

2. <http://cryptome.org/>
3. <http://cryptome.org/nsa-program.htm>
4. <http://btobsearch.barnesandnoble.com/booksearch/isbninquiry.asp?btob=Y&endeca=y&cds2Pid=154&isbn=0743270665>
5. <http://www.fas.org/irp/nsa/quest.pdf>
6. <http://www.nsa.gov/publications/publi00043.pdf>
7. <http://technorati.com/tag/NSA>
8. <http://technorati.com/tag/intelligence>
9. <http://technorati.com/tag/eavesdropping>
10. <http://technorati.com/tag/CIA>

31

### **Security quotes : a FSB (successor to the KGB) analyst on Google Earth (2006-01-04 13:38)**

[1]"Lt. Gen. Leonid Sazhin, an analyst for the Federal Security Service, the Russian security agency that succeeded the K.G.B., was quoted by Itar-Tass as saying: "Terrorists don't need to reconnoiter their target. Now an American

company is working for them." A great [2]quote, and I find it totally true. The point is, not to look for high-resolution imagery, but to harness the power of OSINT, improve their confidence by observing the targets "from the sky", and actually plan and coordinate its activities on huge territories. AJAX anyone? :)

However, the public has always been good at bringing the real issue to the rest of the world.

There have

been [3]numerous [4]attempts to spot sensitive locations, and I wouldn't be myself if I don't share the joys of the

[5]Eyeball Series with you. Of course, in case you haven't come across the initiative earlier.

However, the way it gives terrorists or enemies these opportunities, it also serves the general public by acting as

an evidence for the existence of espionage sentiments, here and there. [6]Echelon's Yakima Research Station was

spotted on GoogleMaps, originally by Cryptome, see the dishes there? Any thoughts in here? Can Microsoft's [7]Local

Live with its highly differentiated bird eye view on important locations turn into a bigger risk the the popularity of

Google's services?

Technorati tags :

[8]Google Earth,[9]Google Maps,[10]satellite imagery,  
[11]OSINT,[12]security,[13]terrorism

1. [http://www.abc.net.au/reslib/200508/r54856\\_148962.jpg](http://www.abc.net.au/reslib/200508/r54856_148962.jpg)

2. <http://www.jsonline.com/bym/news/dec05/379002.asp>

3.  
[http://www.theregister.co.uk/2005/10/14/google\\_earth\\_competition\\_results/](http://www.theregister.co.uk/2005/10/14/google_earth_competition_results/)

4. [http://www.theregister.co.uk/2005/09/13/google\\_earth\\_threatens\\_democracy/](http://www.theregister.co.uk/2005/09/13/google_earth_threatens_democracy/)
5. <http://www.eyeball-series.org/>
6. <http://maps.google.com/maps?q=yakima,+wa&t=k&am;am;am;am;am;am;am;am;am;am;am;am;hl=en&ll=46.682193,-120.356877&spn=0.006801,0.019913&om=1>
7. <http://local.live.com/>
8. <http://technorati.com/tag/Google+Earth>
9. <http://technorati.com/tag/Google+Maps>
10. <http://technorati.com/tag/satellite+imagery>
11. <http://technorati.com/tag/OSINT>
12. <http://technorati.com/tag/security>
13. <http://technorati.com/tag/terrorism>

32

## **How to secure the Internet (2006-01-04 14:22)**

[1]I recently wondered, are there any existing government practices towards securing the entire Internet?

So I went through the [2]U.S National Strategy to Secure Cyberspace, to find out what is the U.S up to given

it still maintains "control" of the Internet. What is the Internet's biggest weakness? No, it's not a sophisticated term, its a common word called design.

A fact that is often neglected as the core of all problems, is that the Net's design by itself was primarily devel-

oped for reseach purposes. That is, universities and scientists exchanging data, users whose activities would

definitely not result in the following :)

- infect the competing Ivy League universities with malware, and "borrow" as much intellectual property as

possible

- Conduct DNS poisoning and redirect their competition's site to their own one

- Eavesdrop on their fellow researcher's communications

The Internet wasn't mean to be as secure as we wished it could be today. So, when it became public and

turned into today's part of daily life, I feel this weakness started to remerge on a harge scale.

Perhaps the second biggest vulnerability is the ability to forge source addresses, and given you can spoof the

origins of your packet no accountability for a great deal of today's threats is present. IPv6 isn't the panacea of

security, and would never be though. There are as a matter of fact a lot of vulnerabilities related to mostly,

implementation, and awareness on the possibilities. But the introduction of IPv6 over the Internet, still remains

an ambition for governments and organizations across the world. As a matter of the the U.S [3]DoD indicated their

troubles while migrating to IPv6, but they desperately [4]need it. Though, I greatly feel the sooner the better.

The current Internet IP space is so easily mapped and datamined, that on most occasions, such transparency is

mostly beneficial to malicious attackers. I believe that security threats can indeed have a national security impact,

of course, given their severity and actual abuse. Today's information and knowledge driven societies are largely

dependent on information and technology infrastructure for most of their needs. This has on the other hand boosted

a tremendous technological growth. It eventually resulted in an increased world productivity, but the dependance

can also affect real life situations on certain occasions.

Can cyberspace indeed influence real-life situations and cause havoc?

Would someone wants to bring down the Internet, and how sound is this? What are the main driving factors behind

33

the known weaknesses of the infrastructure, and how can their negative effects be prevented?

I greatly feel that the growth of E-governments, native Internet population, improved communication infras-

tructure, thus more bandwidth and opportunities, are crucial for the growth of a nation. The only weakness besides

actual usability or utilization, is Security.

Going back to the report, it clearly highlights and takes into consideration both, soft and hard dollars.

That is, enemies conducting espionage over companies, universities, or mapping key government, industry

networks, and easily reachable known targets to be used later on. Hit-lists for potential targets can be easily gathered in today's open source intelligence world.

On a worldwide basis, the implications to the entire Internet posed by insecure DNS servers, and by the inse-

curities of the DNS protocol can undermine the Internet in itself. What happens when all sites are actually there, but

remain unreachable worldwide? The 2002 [5] attacks on the root Internet servers indeed acted as a wake up to the

international community on how fragile the current system really can be.

Some of the obstacles for a secure Internet from my point of view consist of :

- Plain text communications are the easiest, most common way malicious attackers can abuse a nation's com-

munications, excluding the fact that the majority of communications remain unencrypted



- Lack of evolving compliance, threats change so fast, that everyone can barely keep up with them, and what

used to be "secured" yesterday, is vulnerable today

- Less procedures and strategies, more actions, perfecting planning is futile, by the time you end you planning

process you would have to change everything. My point is, empower those who are able to execute real actions

towards improving security.

- The gap between government, private and academic sectors is resulting in a lack of integrated early warning

systems, that would eventually benefit everyone

- Realization of a nationwide client-side sensor, I have also considered Symante's utilization of their 120M

client based as the biggest, most sensitive honeypot ever.

To sum up my ideas, migration to the, at least though to be more secure Internet2 , would take years and

cost billions of dollars on a worldwide basis, yet it's worth it!

34

Have an opinion? Share it!

Technorati tags :

[6]cyberspace,[7]security,[8]information security,[9]IPv6,  
[10]Internet2

1. [http://photos1.blogger.com/blogger/1933/1779/1600/scroll\\_clip.gif](http://photos1.blogger.com/blogger/1933/1779/1600/scroll_clip.gif)
2. [http://www.whitehouse.gov/pcipb/cyberspace\\_strategy.pdf](http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf)
3. <http://www.defenselink.mil/>
4. [http://www.usipv6.com/2003arlington/presents/Marilyn\\_Kraus.pdf](http://www.usipv6.com/2003arlington/presents/Marilyn_Kraus.pdf)
5. <http://www.caida.org/projects/dns-analysis/oct02dos.xml>
6. <http://technorati.com/tag/cyberspace>
7. <http://technorati.com/tag/security>
8. <http://technorati.com/tag/information+security>
9. <http://technorati.com/tag/IPv6>
10. <http://technorati.com/tag/Internet2>

35

## **Happy New Year folks!! (2006-01-04 17:15)**

Dear friends and visitors,

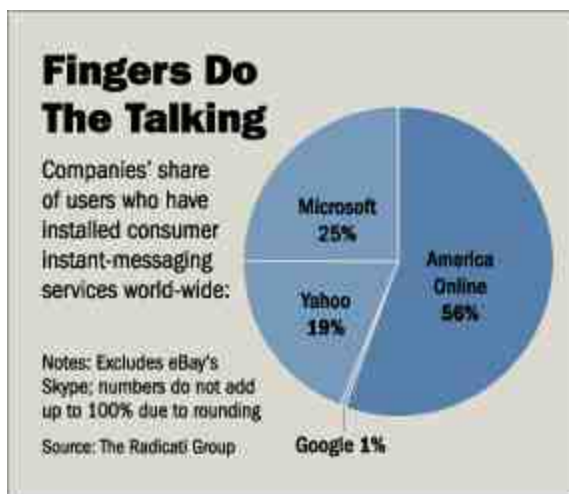
Happy New Year and sincere apologies for the lack of updates on my blog recently. It's not that I have some-

how stopped brainstorming on how to put my knowledge into neat posts, rather, I didn't have the time that I wanted

to provide an in-depth overview of the key topics I had in mind :-)

I wish you all the best in 2006, thank for your feedback on my ideas, and keep ridin' on the road of intellectual exploration!

36



### **What's the potential of the IM security market? Symantec thinks big (2006-01-04 17:17)**

Yesterday, Symantec, one of the world's leading security, and of course, storage providers [1] acquired [2] IMlogic, a

leading provider of Instant Messaging security solutions. How sound is this move anyway? Doesn't Symantec already

have the [3] necessary [4] experience in this field?

IMlogic has never been a build-to-flip company. Dating back to 2002, it has managed to secure important cus-

tomers, Fortune 1000 companies as a matter of fact, and acts as a preferred choice for many of them. And given that

enterprise IM is exploding, and so its home use, the real-time nature of this type of communication has always been

acting as a hit-list in my mind. Client based vulnerabilities, social engineering attacks, auto-responding malware, and

many other issues are among the current trends. How huge is the potential of IM security, or is it me just trying to

think big in here, compared to Symantec's simple product line extension ambition?

Besides acting as another propagation vector for future malware releases, IM usage worldwide is already out-

pacing the most common form of Internet communication - the email. A Radicati Group's research report entitled

"[5]Instant Messaging and Presence Market Trends, 2003-2007" indicates the same. The group [6]predicts that :

[7]

- 1,439 million IM accounts in existence by 2007

- a very significant increase in corporate implementation of IM, from 60 million accounts today to 349 million in 2007.

- that's a degree of monopoly, as always!

Lucky you, Symantec!

With fear of being a pessimist, I have though witnessed how unique organizations and teams got eventually

swallowed by the corporate world. And it's [8]their know-how that I truly miss these days. You can though, still go

through Symantec's constantly updating list of [9]acquired companies, and it's evident they are fully committed to

continue being a market and knowledge leader. I also recommend you read a great article at eWeek entitled [10]IM

Threats : The Dark Side of Innovation to find out more about the current trends. What's your attitude about them?!

Technorati tags :

[11]Symantec, [12]IM, [13]security, [14]information security

1. [http://www.symantec.com/about/news/release/article.jsp?prid=20060103\\_01](http://www.symantec.com/about/news/release/article.jsp?prid=20060103_01)

2. <https://web.archive.org/web/20101103211154/http://www.imlogic.com/>

3. <http://securityresponse.symantec.com/avcenter/reference/secure.instant.messaging.pdf>

4. <https://web.archive.org/web/20101103211154/http://securityresponse.symantec.com/avcenter/reference/threats.to.instant.messaging.pdf>

5. [http://www.ostermanresearch.com/or\\_im05es.pdf](http://www.ostermanresearch.com/or_im05es.pdf)

37

6. [http://online.wsj.com/public/article/SB112907349731466067-fB0n6k6c3HC\\_Kcim4M6p9jHeagE\\_20061011.html?mod=p](http://online.wsj.com/public/article/SB112907349731466067-fB0n6k6c3HC_Kcim4M6p9jHeagE_20061011.html?mod=p)

[ublic\\_home\\_us](#)

7.

[https://web.archive.org/web/20101103211154/http://online.wsj.com/public/resources/images/MK-AF175\\_MSN\\_YA10](https://web.archive.org/web/20101103211154/http://online.wsj.com/public/resources/images/MK-AF175_MSN_YA10)

[112005182104.gif](#)

8. <http://www.atstake.com/>

9.

<http://www.symantec.com/about/profile/development/acquisitions/index.jsp>

10. <http://www.eweek.com/article2/0,1895,1904984,00.asp>

11. <http://technorati.com/tag/Symantec>

12. <http://technorati.com/tag/IM>

13. <http://technorati.com/tag/security>

14. <http://technorati.com/tag/information+security>

38



**Keep your friends close, your intelligence buddies closer! (2006-01-04 17:18)**

[1]

Too much power always leads you to the dark side!

[2]Cryptome has yesterday [3]featured a excerpt from "

[4]State of the War : The Secret History of the CIA and the

Bush Administration" shredding more light on what the NSA used to be before 9/11 and how things changed at a

later stage. In case you really want to find out more about the entire history of the NSA, go though "[5]The Quest for Cryptologic Centralization and the Establishment of NSA, 1940-1952", and some of the most remarkable NSA

released publication entitled "[6]Eavesdropping on Hell : Historical Guide to Western Communications Intelligence and the Holocaust, 1939-1945".

My opinion - With no guards, the gates are always open. But who will watch the watchers when they start watching us?!

Even though, as Marine Corps General Alfred M. Gray have put it years ago "Communications without intelligence is noise, intelligence without communications is irrelevant", and so is privacy in the 21st century, period.

Technorati tags :

[7]NSA, [8]intelligence, [9]eavesdropping, [10]CIA

1. <https://web.archive.org/web/20101103154218/http://www.tl.io.demon.co.uk/eyesky.jpg>
2. <http://cryptome.org/>
3. <http://cryptome.org/nsa-program.htm>
4. <http://btobsearch.barnesandnoble.com/booksearch/isbninqu>

[iry.asp?](#)

[btob=Y&endeca=y&cids2Pid=154&isbn=0743270665](#)

5. <http://www.fas.org/irp/nsa/quest.pdf>
6. <http://www.nsa.gov/publications/publi00043.pdf>
7. <http://technorati.com/tag/NSA>
8. <http://technorati.com/tag/intelligence>
9. <http://technorati.com/tag/eavesdropping>
10. <http://technorati.com/tag/CIA>

39



### **Security quotes : a FSB (successor to the KGB) analyst on Google Earth (2006-01-04 17:19)**

[1]

"Lt. Gen. Leonid Sazhin, an analyst for the Federal Security Service, the Russian security agency that succeeded

the K.G.B., was quoted by Itar-Tass as saying: "Terrorists don't need to reconnoiter their target. Now an American

company is working for them." A great [2]quote, and I find it totally true. The point is, not to look for high-resolution imagery, but to harness the power of OSINT, improve their confidence by observing the targets "from the sky", and actually plan and coordinate its activities on huge territories. AJAX anyone? :)



However, the public has always been good at bringing the real issue to the rest of the world. There have been

[3]numerous [4]attempts to spot sensitive locations, and I wouldn't be myself if I don't share the joys of the [5]Eyeball Series with you. Of course, in case you haven't come across the initiative earlier. However, the way it gives terrorists or enemies these opportunities, it also serves the general public by acting as an evidence for the existence of

espionage sentiments, here and there. [6]Echelon's Yakima Research Station was spotted on GoogleMaps, originally

by Cryptome, see the dishes there? Any thoughts in here? Can Microsoft's [7]Local Live with its highly differentiated

bird eye view on important locations turn into a bigger risk the the popularity of Google's services?

Technorati tags :

[8]Google Earth,[9]Google Maps,[10]satellite imagery, [11]OSINT,[12]security,[13]terrorism

1.  
[https://web.archive.org/web/20101103203555/http://www.abc.net.au/reslib/200508/r54856\\_148962.jpg](https://web.archive.org/web/20101103203555/http://www.abc.net.au/reslib/200508/r54856_148962.jpg)
2. <http://www.jsonline.com/bym/news/dec05/379002.asp>
3.  
[http://www.theregister.co.uk/2005/10/14/google\\_earth\\_competition\\_results/](http://www.theregister.co.uk/2005/10/14/google_earth_competition_results/)
4.  
[http://www.theregister.co.uk/2005/09/13/google\\_earth\\_threatens\\_democracy/](http://www.theregister.co.uk/2005/09/13/google_earth_threatens_democracy/)

6.

maintains "control" of the Internet. What is the Internet's biggest weakness? No, it's not a sophisticated term, its a common word called design.

A fact that is often neglected as the core of all problems, is that the Net's design by itself was primarily devel-

oped for reseach purposes. That is, universities and scientists exchanging data, users whose activities would

definitely not result in the following :)

- infect the competing Ivy League universities with malware, and "borrow" as much intellectual property as

possible

- Conduct DNS poisoning and redirect their competition's site to their own one

- Eavesdrop on their fellow researcher's communications

The Internet wasn't mean to be as secure as we wished it could be today. So, when it became public and

turned into today's part of daily life, I feel this weakness started to remerge on a harge scale.

Perhaps the second biggest vulnerability is the ability to forge source addresses, and given you can spoof the

origins of your packet no accountability for a great deal of today's threats is present. IPv6 isn't the panacea of

security, and would never be though. There are as a matter of fact a lot of vulnerabilities related to mostly,

implementation, and awareness on the possibilities. But the introduction of IPv6 over the Internet, still remains

an ambition for governments and organizations across the world. As a matter of the the U.S [3]DoD indicated their

troubles while migrating to IPv6, but they desperately [4]need it. Though, I greatly feel the sooner the better.

The current Internet IP space is so easily mapped and datamined, that on most occasions, such transparency is

mostly beneficial to malicious attackers. I believe that security threats can indeed have a national security impact,

of course, given their severity and actual abuse. Today's information and knowledge driven societies are largely

dependent on information and technology infrastructure for most of their needs. This has on the other hand boosted

a tremendous technological growth. It eventually resulted in an increased world productivity, but the dependance

can also affect real life situations on certain occasions.

Can cyberspace indeed influence real-life situations and cause havoc? Would someone wants to bring down

42

the Internet, and how sound is this? What are the main driving factors behind the known weaknesses of the infrastructure, and how can their negative effects be prevented?

I greatly feel that the growth of E-governments, native Internet population, improved communication infras-

structure, thus more bandwidth and opportunities, are crucial for the growth of a nation. The only weakness besides

actual usability or utilization, is Security.

Going back to the report, it clearly highlights and takes into consideration both, soft and hard dollars. That is,

enemies conducting espionage over companies, universities, or mapping key government, industry networks, and

easily reachable known targets to be used later on. Hit-lists for potential targets can be easily gathered in today's

open source intelligence world.

On a worldwide basis, the implications to the entire Internet posed by insecure DNS servers, and by the inse-

curities of the DNS protocol can undermine the Internet in itself. What happens when all sites are actually there, but

remain unreachable worldwide? The 2002 [5] attacks on the root Internet servers indeed acted as a wake up to the

international community on how fragile the current system really can be.

Some of the obstacles for a secure Internet from my point of view consist of :

- Plain text communications are the easiest, most common way malicious attackers can abuse a nation's com-

munications, excluding the fact that the majority of communications remain unencrypted

- Lack of evolving compliance, threats change so fast, that everyone can barely keep up with them, and what

used to be "secured" yesterday, is vulnerable today

- Less procedures and strategies, more actions, perfecting planning is futile, by the time you end you planning

process you would have to change everything. My point is, empower those who are able to execute real actions

towards improving security.

- The gap between government, private and academic sectors is resulting in a lack of integrated early warning

systems, that would eventually benefit everyone

- Realization of a nationwide client-side sensor, I have also considered Symante's utilization of their 120M

client based as the biggest, most sensitive honeypot ever.

To sum up my ideas, migration to the, at least though to be more secure Internet2 , would take years and

cost billions of dollars on a worldwide basis, yet it's worth it!

Have an opinion? Share it!

Technorati tags :

[6]cyberspace,[7]security,[8]information security,[9]IPv6,  
[10]Internet2

1.

[https://web.archive.org/web/20101103204440/http://photos1.blogger.com/blogger/1933/1779/1600/scroll\\_clip.g](https://web.archive.org/web/20101103204440/http://photos1.blogger.com/blogger/1933/1779/1600/scroll_clip.g)

[if](#)

2.

[http://www.whitehouse.gov/pcipb/cyberspace\\_strategy.pdf](http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf)

3. <http://www.defenselink.mil/>

4.

[http://www.usipv6.com/2003arlington/presents/Marilyn\\_Kraus.pdf](http://www.usipv6.com/2003arlington/presents/Marilyn_Kraus.pdf)

5. <http://www.caida.org/projects/dns-analysis/oct02dos.xml>

6. <http://technorati.com/tag/cyberspace>

43

7. <http://technorati.com/tag/security>

8. <http://technorati.com/tag/information+security>

9. <http://technorati.com/tag/IPv6>

10. <http://technorati.com/tag/Internet2>

44



## **Malware - future trends (2006-01-09 17:22)**

[1]

I'm very excited to let you know that, I have finally managed to release my [2]"Mal-

ware - future trends" publication. Basically, it will provide you with an overview of the current trends, the driving

factors behind the scene, and some of the trends to come, from my point of view.

**As factors contributing to the rise and success of malware I have pointed out :**

- Documentation and howto's transformed into source code
- Vulnerabilities, even patches, easily turned into exploits
- Clear signs of consolidation on the malware scene
- The media as a fueling factor for growth
- Over 960M unique Internet users and their connectivity, or purchasing power
- The demand for illegal services

**And as far as the trends themselves are concerned, I have indicated :**

- Mobile malware will be successfully monetized
- Localization as a concept will attract the coders' attention
- Open Source Malware
- Anonymous and illegal hosting of (copyrighted) data
- The development of Ecosystem
- Rise in encryption and packers
- 0day malware on demand
- Cryptoviral extortion / Ransomware will emerge



- When the security solutions (antivirus etc.) ends up the security problem itself
- Intellectual property worms
- Web vulnerabilities, and web worms - diversity and explicit velocity
- Hijacking botnets and infected PCs
- Interoperability will increase the diversity and reach of the malware scene

Have an opinion?

Feel I have somehow missed a point? Let me know, or directly comment on this post!

Thanks folks!

Technorati Tags :

[3]malware,[4]antivirus,[5]security,[6]information security,  
[7]malware trends,[8]viruses

1. <https://web.archive.org/web/20101103212014/http://photos1.blogger.com/blogger/1933/1779/1600/Image38.jpg>

2. <http://www.packetstormsecurity.org/papers/general/malware-trends.pdf>

3. <http://technorati.com/tag/malware>

4. <http://technorati.com/tag/antivirus>

5. <http://technorati.com/tag/security>

6. <http://technorati.com/tag/information+security>

7. <http://technorati.com/tag/malware+trends>

45

8. <http://technorati.com/tag/viruses>

46



### **Watch out your wallets! (2006-01-10 17:24)**

[1]

The irony of today's, obviously not working loan system, has left a 22 years old

Chicago student in [2]debt of \$412,000. A very scary event, that I feel could have been prevented if the loss was

reported, and the bank giving the loans was somehow aware of the social status of the "borrower" :)

In case you are interested in knowing more about identity theft, go through the following :

[3]ID Theft : When Bad Things Happen to Your Good Name

[4]Coping with Identity Theft : Reducing the Risk of Fraud

[5]The Problem of Identity Theft

Technorati tags :

[6]identity theft,[7]security,[8]information security,[9]fraud

1.

<https://web.archive.org/web/20101103164540/http://www.iwar.org.uk/ecoespionage/resources/id-theft/idtheft.pdf>

[pdf](#)

2. <http://www.upi.com/NewsTrack/view.php?StoryID=20060108-054533-4750r>

3. <http://www.ftc.gov/bcp/online/pubs/credit/idtheft.pdf>

4. <http://www.privacyrights.org/fs/fs17-it.htm>

5. <http://www.popcenter.org/Problems/PDFs/Identity%20Theft.pdf>

6. <http://technorati.com/tag/identity+theft>

7. <http://technorati.com/tag/security>

8. <http://technorati.com/tag/information+security>

9. <http://technorati.com/tag/fraud>

47



## **Would we ever witness the end of plain text communications? (2006-01-10 17:25)**

[1]

Last week, a report released by the research firm In-Sat estimated that [2]revenues for IP VPNs will double between 2004 and 2009 to \$658 million.

Estimates should also be questioned, though the trend is very relevant these days. VPNs as a concept are the natural shift from avoiding plain text data exchange over the insecure by default Internet. Yet, secure communication channel doesn't mean actual attacks on the both, the channel and the host itself cannot be executed. Though, I think that avoiding plain text communications at all is a strategic step of a great important.

### **How you can take advantage of this trend?**

Given the market is actively growing, namely a lot of new entrants, it would mean a lot of product/service choice and very competitive pricing schemes. Keep track of them, and ensure your TOC is as low as possible, think in the long-term.

### **What to keep in mind?**

Do your homework, and while a newly established company offers might seem attractive compared to an

established vendor's one in respect to pricing, don't ignore expertise and quality for a short-term deal. On the other

hand, make sure you are aware of the fact, that vendors will rush into offering many other cross-sale services. We

are already witnessing such vendors being as confident as to launch their own anti-virus solutions. That's exactly the

type of companies whose product extension services you should avoid, as they are basically reinventing the wheel,

with the idea to cut paying any royalties to the established anti virus vendors. TOC, expertise, value oriented and

flexible vendors are the things to keep in mind, given you don't have something else in mind?

Technorati tags :

48

[3]VPN, [4]security,[5] information security, [6]secure communications

1. [https://web.archive.org/web/20101103160616im\\_/http://www.svtarot.com/net/encryption.gif](https://web.archive.org/web/20101103160616im_/http://www.svtarot.com/net/encryption.gif)
2. <http://www.networkingpipeline.com/security/175801374>
3. <http://technorati.com/tag/VPN>
4. <http://technorati.com/tag/security>
5. <http://technorati.com/tag/information+security>
6. <http://technorati.com/tag/secure+communications>

49



## **Why we cannot measure the real cost of cybercrime? (2006-01-10 17:28)**

[1]

At the end of 2005, a rather contradictive statement was made,

namely, that the [2]costs of cybercrime have surpassed those of drug smuggling? And while I feel it has been made

in order to highlight the threats posed by today's cyber insecurities, I find it a bit of an unrealistic one.

Mainly because of :

**- the lack of centralized database and approach to keep track of, and measure the costs of cyber crime**

Centralization is useful sometimes, and so is standardization. My point is that, doesn't matter how many metrics I go

through on a monthly basis. They all have had different approaches while gathering their data. Estimated or

projected loses are a tricky thing the way [3]Donald Trump's valuation is largely based on his name brand. In this

very same way, if we were to quantify the losses of a worldwide worm outbreak posed by direct attacks of the

availability and integrity of networks and hosts, it would always be rather unrealistic, yet hopefully scientifically

justified to a certain extend!

I feel it's about time the industry appoints a watchdog with an in-depth understanding of the concept. A watchdog

that has the open source intelligence attitude, and the law enforcement backup to differentiate online identity theft

next to dumpest diving, and both, soft and hard dollar losses out of an event.

## **- the flawed approaches towards counting the TOC costs**

"We had our network hit by a worm attack, where 200 out of 1000 desktops got successfully infected resulting in 4

hours downtime of the 200 desktops, and with the department's \$15 hourly rate it resulted in direct loss of

productivity." Rather common approach these days, what isn't included is the time the IT/Security department

spent fixing the problem, the eventually

increased infosec budget (given the department takes advantage of the momentum and asks for more), and and

potential law suits that may follow by other companies whose systems have been attacked by any of the 200

infected ones. A security incident shouldn't be isolated when it comes to costs, yet it's the best approach to bring

some accountability, though, it's totally unrealistic. The butterfly effect has its word in both the real, and the

financial world as well.

## **- the hard to quantify intellectual property theft**

Continuing my thoughts from the abovementioned opinion, if we were to count the IT/Security department's

associated costs, as well as the loss of productivity next to the hourly rate, especially when there's been a theft of

intellectual property is easy, yet, untrue. If we were to even estimate the potential dollar losses of intellectual property theft due to security breaches, it would surpass the U.S budget's deficit and reach levels of a developing economy's GDP, I bet that! The current inability of the industry

to successfully quantify the costs of intellectual property theft, results in a mere estimation of the real costs of the cyber crime act. In this case, it's more complex that some want to believe.

### **- lack of disclosure enforcement**

More and more states(U.S only, painfully true but the world is lacking behind) are adopting breach disclosure laws

with the idea to prevent successful use of the information, seek accountability from the organizations/enterprises,

and, hopefully result in even more clear metrics on what exactly is going on in the wild. However, the lack of

acceptance, and sometimes,

even the awareness of being hacked is resulting into the highly underestimated, and actual picture in respect to the

real state of cyber crime today. The more disclosure enforcement, and actual awareness of the breaches, the better

the metrics, understanding of where the threats are going, and accountability for the organizations themselves.



**- survey and metrics should always be a subject to question**

The way a research company gathers survey and metrics data should always be a subject to questions. Even highly respected law enforcement agencies surveys and research, clearly indicate similarities, though when it comes to financial losses, every organization has a different measurement approaches and understanding of the concept.

That is why, in the majority of cases, they aren't even aware of the actual long-term, or soft dollar losses directly

posed by a single security breach. Evaluating assets, and assigning dollar values to intellectual property is tricky, and it could both, provide a more realistic picture of the actual losses, or overestimate

them due to the company "falling in love" with the intellectual value of its breached information.

**- companies fearing shame do not report the most relevant events today, online extortion or DDoS attacks**

No company would publicly admit complying with online extortionists, and no matter how unprofessional it may

sound, a LOT of companies pay not to have their reputation damaged, and it's not just public companies I'm talking

about. How should a company react in such a situation, fight back, have it's web site shut down resulting in direct \$

losses outpacing the sum requested by extortionists, or complying with the request, to later on having to deal with

issue again? How much value would a company gain for fighting back, or for publicly stating of having such a

problem, and complying with it? What's more, should quantifying a successful DDoS attack on a E-shop also include

the downtime effect for the ISP's customers, given they don't null route

the site of course? And who's counting all these counts, and how far would their impact actually reach?

### **- the umatelized sales of people avoiding shopping online**

A topic that is often neglected when it comes to E-commerce, is the HUGE number of people that aren't interested

in participating(though they have the E-ability to do so), mainly because of the fear posed by cyber crime, having

their credit card data stolen etc. The current revenues of E-commerce in my point of view, are nothing compared to

what they could be given the industry's leaders gently unite in order to build awareness on their actions towards

improving security. I also consider these people as a cost due to cyber crime!

At the bottom line, drug addicts don't exist because of drugs, but because of the society, and it may be easier to

execute phishing attacks than smuggle cocaine from Mexico to the U.S, but this is where the real \$ \$ \$ truly is from

my point of view - drugzZzZzZzZ.....:)

Technorati tags :

[4]cybercrime,[5]security,[6]information security,[7]ROSI

1.  
[https://photos1.blogger.com/blogger/1933/1779/1600/0323\\_118bit.gif](https://photos1.blogger.com/blogger/1933/1779/1600/0323_118bit.gif)

51

2.  
[http://money.cnn.com/2005/12/29/technology/computer\\_security/index.htm](http://money.cnn.com/2005/12/29/technology/computer_security/index.htm)

3. <http://www.trump.com/>

4. <http://technorati.com/tag/cybercrime>

5. <http://technorati.com/tag/security>

6. <http://technorati.com/tag/information+security>

7. <http://technorati.com/tag/ROSI>

52



**The never-ending "cookie debate" (2006-01-10 17:30)**

[1]

On the 6th of January, CNET reported that the web sites of 23 U.S senators use [2]persistent cookies (usually expiring around 2035), and several days earlier, [3]Google-Watch.org found out the same for [4]NSA's web site.

[5]

As a matter of fact, Google, the world's most popular search engine with millions of searches in over 100 languages,

also uses cookies that [6]expire in 2035. But how does this all matter to you? Does erasing your cookies makes you

invisible, invincible and not traceable?

Totally wrong! However, cookies are the most popular privacy invading concept on the Internet, and if you start

filling in privacy conscious individuals into the basics of timing attacks, [7]remote physical devices fingerprinting, or distributed surveillance possibilities, they'll end up thinking you're paranoid - for a reason!

What you MUST know concerning your privacy on the Internet is that, in today's globalized Internet, namely

hundreds of countries participating, privacy laws, their enforcement or even understand of the important of the

issue, tend to vary from country to country.

There are worst things that could happen to you compared to cookies, and I refer to them as [8]Web Timing Attacks,

and how [9]practical they really are! Don't bother about cookies, given you wiped them out, that's the [10]Cookie

Monster's job :)

In case you are interested in further info on the topic you can take a look at the following :

[11]How Web Server's Cookies Threaten Your Privacy

[12]Local Shared Objects - "Flash Cookies"

[13]EPIC's Cookies Page

[14]Search Privacy At Google & Other Search Engines

[15]Bugnosis

[16]Taking the Byte Out of Cookies

Technorati tags :

[17]cookies, [18]persistent cookies, [19]privacy,  
[20]security, [21]information security

1.

<https://photos1.blogger.com/blogger/1933/1779/1600/cookiemonster.0.jpg>

2.

[http://news.com.com/Congress+hands+caught+in+the+cookie+jar/2100-1028\\_3-6020711.html?tag=cd.top](http://news.com.com/Congress+hands+caught+in+the+cookie+jar/2100-1028_3-6020711.html?tag=cd.top)

3. <http://www.google-watch.org/>

4. <http://www.google-watch.org/nsacook.html>

5.

<https://web.archive.org/web/20101103191948/http://photos1.blogger.com/blogger/1933/1779/1600/cookiemonster>

53

.0.jpg

6. <http://www.google-watch.org/cgi-bin/cookie.htm>
7. <http://www.caida.org/outreach/papers/2005/fingerprinting/KohnoBroidoClaffy05-devicefingerprinting.pdf>
8. <http://www.cs.princeton.edu/sip/pub/webtiming.pdf>
9. <http://crypto.stanford.edu/~dabo/papers/ssl-timing.pdf>
10. [http://en.wikipedia.org/wiki/Cookie\\_Monster](http://en.wikipedia.org/wiki/Cookie_Monster)
11. <http://www.junkbusters.com/cookies.html>
12. <http://epic.org/privacy/cookies/flash.html>
13. <http://www.epic.org/privacy/internet/cookies/>
14. <http://searchenginewatch.com/sereport/article.php/2189531>
15. <http://www.bugnosis.org/>
16. <https://draft.blogger.com/http://cpe.njit.edu/dlnotes/CIS/CIS350/TakingTheByteOutOfCookies.pdf>
17. <http://technorati.com/tag/cookies>
18. <http://technorati.com/tag/persistent+cookies>
19. <http://technorati.com/tag/privacy>
20. <http://technorati.com/tag/security>

21. <http://technorati.com/tag/information+security>

54

### **The hidden internet economy (2006-01-11 17:39)**

How much does phishing, spam and spyware for instance cost on businesses? Should we measure in cash, or hardly

quantified long-term affects such as reputation damage, loss of confidence in the business, or the percentage of

people that would think twice before doing any E-shopping at all?

These days, I believe that there's a huge number of individuals with purchasing power that tend to avoid online

purchases at all. That's the baby boomers I am talking about, who as a matter of fact are having more and more

disposable income!

Published in December, 2005, a poll published by the [1]CSIA estimated that almost 50 % of all adults in the U.S

avoid making purchases online because they are afraid that their personal information could be stolen. And while

impulsive teens are excluded, and the poll's quality is taken for granted, to me it highlights an important fact that I

have always believed in - that there is a hidden Internet economy that could boom given more confidence is build in

ensuring that, this huge number of individuals will start bringing even more online revenues to any of the dotcom

darlings. Until then, stay tuned for yet another major security breach at a data aggregator :(

Technorati tags :

[2]internet economy, [3]dotcom, [4]security, [5]information security, [6]CSIA

1. <https://www.csalliance.org/>
2. <http://technorati.com/tag/internet+economy>.
3. <http://technorati.com/tag/dotcom>
4. <http://technorati.com/tag/security>.
5. <http://technorati.com/tag/information+security>
6. <http://technorati.com/tag/CSIA>





## **Security threats to consider when doing E-Banking (2006-01-12 17:40)**

[1]

E-banking, and mobile commerce are inevitable part of our daily lifes, and would continue to get more popular.

The bad thing is, that it's not just us, the end users benefiting from this fact, but also, the malicious attackers exploiting our naivety and lack of awareness on the threats to watch for. [2]Candid Wuuest did an outstanding [3]research on

the insecurities of E-banking, and excellect job in comparing the different security measures next to one another. The

[4]slides will also provide you with a lot of useful info on the topic.

Further info on the topic can also be found at :

[5]Why eBanking is Bad for your Bank Balance

[6]Risk management principles for electronic banking

Technorati tags :

[7]e-banking, [8]electronic banking,[9] E-commerce,[10] security, [11]information security

1. [https://photos1.blogger.com/blogger/1933/1779/1600/100302\\_internet\\_banking.0.jpg](https://photos1.blogger.com/blogger/1933/1779/1600/100302_internet_banking.0.jpg)
2. <http://www.wueest.ch/>
3. <http://www.astalavista.com/index.php?section=directory&linkid=5659>
4. <http://www.aavar.org/avar2005/speech/020.ppt>
5. [http://www.ebankingsecurity.com/ebanking\\_bad\\_for\\_your\\_bank\\_balance.pdf](http://www.ebankingsecurity.com/ebanking_bad_for_your_bank_balance.pdf)
6. <http://www.bis.org/publ/bcbs98.pdf>
7. <http://technorati.com/tag/e-banking>
8. <http://technorati.com/tag/electronic+banking>
9. <http://technorati.com/tag/E-commerce>
10. <http://technorati.com/tag/security>
11. <http://technorati.com/tag/information+security>

### **Insecure Irony (2006-01-12 17:42)**

What's the worst thing that could happen to [1]BigBrother and any of its puppets? – Have their [2]confidential info

exposed due to the negligence of a commercial organization, one that is used for gathering the majority of intelligence

data these days. Now, that's an insecure irony.

It is a public secret that any government is gathering enormous information on its citizens through commercial orga-

nization's extremely rich databases. Everyone's in the system though, even the ghosts!

I also advise you to go through a great research on the topic of "[3]Commercial Data and National Security" in case you want to know more on how governments and intelligence agencies use/abuse the data.

Technorati tags :

[4]bigbrother,[5]surveillance,[6]privacy,[7]security breach,[8]security,[9]information security

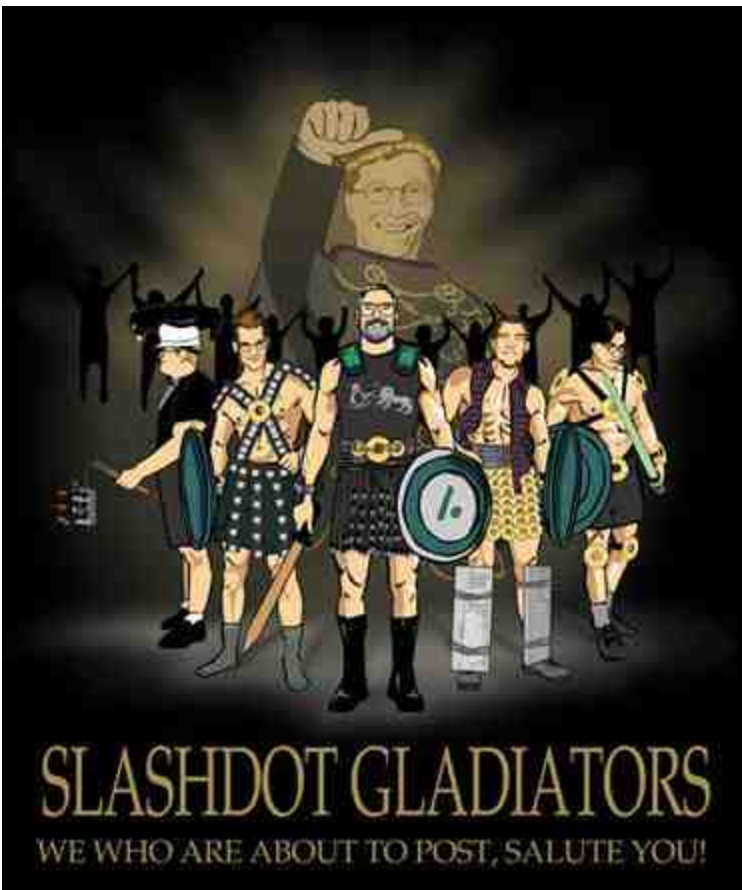
1. [http://en.wikipedia.org/wiki/Big\\_Brother\\_%281984%29](http://en.wikipedia.org/wiki/Big_Brother_%281984%29)

2. <https://web.archive.org/web/20101016193525/http://www.eweek.com/article2/0,1759,1907936,00.asp>

3. <http://www.cdt.org/publications/200408dempseyflint.pdf>

4. <http://technorati.com/tag/big+brother>
5. <http://technorati.com/tag/surveillance>
6. <http://technorati.com/tag/privacy>
7. <http://technorati.com/tag/security+breach>
8. <http://technorati.com/tag/security>
9. <http://technorati.com/tag/information+security>

57



**Future Trends of Malware (2006-01-16 17:43)**

[1]

Great news, that I greatly anticipated, my "[2]Malware - Future Trends" research got [3]Slashdotted. The strange thing is how my actual post and numerous others from different respected sites weren't approved. I guess I would have to

live with that, given the huge number of hits and new subscribers to my [4]feed I have received for the last couple of

days :))

Someone once said, that it's all about to courage to write down what you think. And he was right, but he missed to

mention, that you should also stand behind what you believe in. There's nothing more important than disseminating

that kind of information to the broadest audience possible, in the fastest way achievable. The comments, links

recognition and active feedback that I have been receiving, are the best benchmark for the usefulness of my research.

So, thanks!

My "Malware - future trends" publication has recently appeared at :

[5]Packetstormsecurity.org

[6]Securiteam.com

[7]Net-security.org

[8]LinuxSecurity.com

[9]Infosecwriters.com

[10]WhiteDust.net

[11]ISECA.org

[12]BankInfoSecurity.com

[13]Wiretapped.net

[14]Astalavista.com

58

[15]CGISecurity.com

[16]Megasecurity.org

[17]Secguru.com

[18]Wikipedia's entry on Malware

to name few of the sites, and in various blog comments :

[19]Computerworld's IT Management Blog

[20]Datamation's Blog

[21]Sergio Hernando's post, and the [22]Google translation

[23]Alan Cardel's Blog

[24]Worm Blog

And many others : [25]1, [26]2, [27]3, [28]4, [29]5, [30]6,  
[31]7, [32]8, [33]9, [34]10, [35]11, [36]12, [37]13,

[38]14, [39]15, [40]16, [41]17, [42]18, [43]19, [44]20

The more naysayers, the more important is what you are doing, and I have come across a lot of them, though

I wouldn't even bother to link them back. They are a valuable incentive on a certain occasions. It's a great feeling that I missed for a little while, it reminds of the how differently people react to one another's success and hard work.

I totally enjoy people quoting me on every sentence from a 26 pages publication I pretty much finalized on Xmas eve, just for the idea of doing it.

Cheer up, guys, and go through my points objectively.

What I truly like, is the debate it opened up here and there, one of the main ideas behind it. Feel free to post

your comments at my original announcement, [45]Malware - Future Trends.

Technorati tags :

[46]Slashdotted,[47]slashdot,[48]malware trends,  
[49]malware,[50]security,[51]information security

1.

<https://www.geekculture.com/geekculturestore/webstore/webstoreimages/slashdotgladiators/gladiatorbig.jpg>

2.

<http://www.packetstormsecurity.org/papers/general/malware-trends.pdf>

3. <http://it.slashdot.org/it/06/01/11/1323212.shtml>

4. <http://feeds.feedburner.com/DanchoDanchevOnSecurityAndNewMedia>
5. <http://www.packetstormsecurity.org/filedesc/malware-trends.pdf.html>
6. <http://www.securiteam.com/securityreviews/5IP0B0AHFA.html>
7. <http://www.net-security.org/article.php?id=891>
8. <http://www.linuxsecurity.com/content/view/121194/49/>
9. <http://www.infosecwriters.com/texts.php?op=display&id=390>
10. [http://www.whitedust.net/article/45/Future\\_Trends\\_of\\_Malware/](http://www.whitedust.net/article/45/Future_Trends_of_Malware/)
11. <http://www.iseca.org/modules/mydownloads/visit.php?cid=50&lid=86>
12. [http://www.bankinfosecurity.com/whitepapers.php?wp\\_id=42](http://www.bankinfosecurity.com/whitepapers.php?wp_id=42)
13. <http://www.mirrors.wiretapped.net/security/info/papers/malware/danchev-2006--malware-trends.pdf>
14. <http://astalavista.com/index.php?section=directory&cmd=detail&id=5921>
15. <http://www.cgisecurity.com/2006/01/05>
16. <http://www.megasecurity.org/papers/malwaretrends.pdf>



17. [http://www.secguru.com/malware\\_future\\_trends](http://www.secguru.com/malware_future_trends)
18. <http://en.wikipedia.org/wiki/Malware>
19. <http://www.computerworld.com/blogs/node/1562>
20. [http://blog.datamation.com/blog/archives/2006/01/whats\\_ah\\_ead\\_for.html](http://blog.datamation.com/blog/archives/2006/01/whats_ah_ead_for.html)
- 59
21. <http://www.sahw.com/wp/archivos/2006/01/10/tendencias-futuras-en-el-malware/>
22. [http://www.google.com/translate?  
u=http://www.sahw.com/wp/archivos/2006/01/10/tendencia  
s-futuras-en-el-mal  
ware/&langpair=esen&amp;amp;amp;amp;amp;a  
mp;](http://www.google.com/translate?u=http://www.sahw.com/wp/archivos/2006/01/10/tendencia-s-futuras-en-el-malware/&langpair=esen&amp;amp;amp;amp;amp;a mp;)
23. <http://alancalder.blogspot.com/2006/01/future-trends-of-malware.html>
24. [http://www.wormblog.com/2006/01/malware\\_future\\_.html](http://www.wormblog.com/2006/01/malware_future_.html)
25. <http://micheladrien.blogspot.com/2006/01/report-on-future-trends-in-malware.html>
26. <http://bhayden.blogspot.com/2006/01/whitedust-future-trends-of-malware.html>
27. <http://www.thenetworksecurity.org/news/article-350.html>
28. <http://waterloosystems.net/news/?p=114>

29. <http://www.livejournal.com/users/defconfunk/100065.html>
30. <http://www.jbiz.com/2006/01/future-trends-of-maleware.html>
31. <http://triptronix.net/ishbadiddle/archives/2006/01/11/13.55.48/default.asp>
32. [http://www.kross.ro/malware\\_future\\_trends](http://www.kross.ro/malware_future_trends)
33. <http://del.icio.us/url/75f17b61ad70d2dd06d75e56d5588123>
34. <http://cofradia.org/modules.php?name=News&amp;file=article&sid=16261>
35. <http://www.bespacific.com/mt/archives/010102.html#010102>
36. <http://www.hackerscenter.com/archive/view.asp?id=21737>
37. <http://newsvac.newsforge.com/newsvac/06/01/12/1554243.shtml>
38. <http://reviews.cnet.com/5208-6132-0.html?forumID=32&threadID=149179&messageID=1663363>
39. <http://www.securitycurve.com/blog/archives/000321.html>

40. <http://www.windowsecurity.com/whitepapers/Malware-future-trends.html>
41. <http://security.ittoolbox.com/white-papers/Malware-Future-Trends-5222>
42. [http://www.security.nl/article/12808/1/De\\_toekomst\\_van\\_malware.html](http://www.security.nl/article/12808/1/De_toekomst_van_malware.html)
43. <http://bezpeka.com/en/lib/antispay/anot2870.html>
44. <http://www.reseaux-telecoms.net/actualites/lire-bientot-le-virus-et-l-attaque-dos--on-demand-12182.html>
45. <http://ddanchev.blogspot.com/2006/01/malware-future-trends.html>
46. <http://technorati.com/tag/Slashdotted>
47. <http://technorati.com/tag/slashdot>
48. <http://technorati.com/tag/malware+trends>
49. <http://technorati.com/tag/malware>
50. <http://technorati.com/tag/security>
51. <http://technorati.com/tag/information+security>

60

### **To report, or not to report? (2006-01-16 17:45)**

[1]Computerworld is running a story that, “[2]Three more U.S states add laws on data breaches”, but what would be

the consequences of this action? Less security breaches? I doubt so. Realistic metrics and reactions whenever an

actual breach occurs, as well as its future prevention measures? Now that's something I think.

Such [3]legislations have a huge impact, both, on the industry, the public opinion, and company itself. No one

likes admitting getting hacked, or having sensitive information exposed to unknown and obviously malicious party.

Yet, if it wasn't companies reporting these breaches, thousands of people would have been secretly exposed to

possible identity theft, and we'll be still living with the idea that the [4]Megacorporations are responsibly handling

our information. Which they obviously aren't! And even if they try to hide it, sooner or later a victim will start

digging in, and the story ends up in mainstream news. [5]Privacyrights.org have taken the time and effort to compile

a "[6]A Chronology of Data Breaches Reported Since the ChoicePoint Incident", and as you can see, it's not getting any better, though, reporting and legislations have the potential to change a lot.

At the bottom line, I am a firm believer that, reporting breaches greatly improves the accuracy of security metrics,

and hopefully the solutions themselves. Security through obscurity is simply out of question when it comes to

storing unencrypted databases online, or even distributing them offline, though, it's still obviously very popular today.

What do you think? Are the long-term negative PR effects worth the uninterrupted business continuity as a

whole? Are you comfortable with not knowing how exactly is any of the organizations possessing sensitive info on

you, is taking care to secure it? I'm not!

As well as various other comments on the topic :

[7]Information Security Breaches and the Threat to Consumers

[8]Security Breaches : Notification, Treatment, and Prevention

[9]Recommended Practices on Notification of Security Breach Involving Personal Information

[10]What Does a Computer Security Breach Really Cost?

Technorati tags :

[11]information security,[12]security,[13]security breach,[14]id theft

1. <http://www.computerworld.com/>

2. <http://www.computerworld.com/securitytopics/security/story/0,10801,107574,00.html>

3. <http://www.ncsl.org/programs/lis/CIP/priv/breach.htm>

4. <http://en.wikipedia.org/wiki/Megacorporation>

5. <http://www.privacyrights.org/>
6. <http://www.privacyrights.org/ar/ChronDataBreaches.htm>
7. [http://www.hunton.com/files/tbl\\_s47Details/FileUpload265/1280/Information\\_Security\\_Breaches.pdf](http://www.hunton.com/files/tbl_s47Details/FileUpload265/1280/Information_Security_Breaches.pdf)
8. <http://www.educause.edu/ir/library/pdf/ERM05413.pdf>
9. <http://www.privacy.ca.gov/recommendations/secbreach.pdf>
10. <http://www.avatier.com/files/pdfs/CostsOfBreaches-SANSInstitute.pdf>
11. <http://technorati.com/tag/information+security>
12. <http://technorati.com/tag/security>
13. <http://technorati.com/tag/security+breach>
14. <http://technorati.com/tag/id+theft>

61

## **Anonymity or Privacy on the Internet? (2006-01-16 17:47)**

Last week, [1]Bruce Schneier wrote a great comment on Anonymity, how it won't kill the Internet, and that it has to do with accountability mostly.

Logically, if identification is impossible, then there cannot be adequate accountability. Though, alternative methods

based on the collective trust exist, and are as anonymous, as necessary. Spoofed identities, perhaps even hijacked

ones should also be taken into consideration. But how important is Anonymity today? What is Anonymity and

Privacy anyway? When is the first desired to preserve the second? How blur is the line in between? I think

Anonymity is so much broader than it is originally perceived.

I've once mentioned the possibilities of [2]IP cloaking for competitive intelligence/disinformation. On the other

hand, for me today's concept of anonymity has three dimensions :

**- The individuals trying to achieve anonymity with the idea to express their right of free speech, and access**

**[3]censored information**

A [4]chinese citizen is the first thing that comes to my mind, though many others are having the same problems

when trying to access information or express their right of free speech, such as [5]Saudi Arabia, [6]United Arab

Emirates, [7]Bahrain, [8]Iran, [9]Singapore, [10]Burma, and [11]Tunisia.

**- Those trying to avoid accountability for certain actions, in one way or another**

[12]Anonymous-p2p.org has for instance featured a list of P2P applications that improve anonymity to a certain

extend. In this case, anonymity is desired in order to cover up certain actions. The use of proxy servers to try to hide originating host should also be mentioned as a possibility.

**- Those with an established pseudo-anonymity, netizens for instance**

I think pseudo-anonymity is important in today's society, it's utopian worlds(online gaming worlds etc.), express

freedom and promote creativity to a certain extend. The entire trust and accountability model is actually entrusted

on the service, for instance, Ebay as mentioned in the original article. You trust that Ebay's practices going beyond

this pseudo-anonymity would achieve accountability in case it's necessary.

What others think on privacy, and why is anonymity hard?

"[13] *There's no Privacy, get over it*" Sun's CEO **Scott McNealy**, back in 1999

**John Young**, [14]Cryptome.org [15]on privacy, data aggregation, data mining, terrorism fears and our constantly

digitized lives :

*"Privacy should be a right of citizens worldwide, in particular the right to keep government and business from gaining access to private information and personal data. The argument that government needs to violate privacy in order to*

*assure security is a lie. The business of gathering private information by corporations and then selling that to*



*government and other businesses is a great threat to civil liberties. Much of this technology was developed for*

*intelligence and military uses but has since been expanded to include civil society. "*

Dan Farmer and Charles C.Mann – [16]Surveillance Nation

*"Low-priced surveillance technologies will help millions of consumers protect their property, plan their commutes,*

62

*and monitor their families. But as these informal intelligence-gathering networks overlap and invade our privacy, that very could evaporate."*

Does Privacy still exist in the 21st century? Is Anonymity an excuse for Privacy? What do you think?

Further resources on privacy and anonymity can also be found at :

[17]Real World Patterns of Failure in Anonymity Systems

[18]Better Anonymous Communications

[19]Introduction to P3P

[20]HOWTO bypass Internet Censorship

[21]Formalizing Anonymity - A Review

[22]Anonymity made easy

[23]Anonymity and Pseudonymity in Cyberspace  
:Deindividuation, Incivility and Lawlessness Versus Freedom  
and

## Privacy

Technorati tags :

[24]privacy,[25]anonymity,[26]censorship,[27]free speech,  
[28]digital rights

1. <http://www.wired.com/news/columns/0,70000-0.html>
2. <http://ddanchev.blogspot.com/2005/12/ip-cloaking-and-competitive.html>
3. <http://en.wikipedia.org/wiki/Censorship>
4. [https://web.archive.org/web/20101016193525/http://www.opennetinitiative.net/studies/china/ONI\\_China\\_Country\\_Study.pdf](https://web.archive.org/web/20101016193525/http://www.opennetinitiative.net/studies/china/ONI_China_Country_Study.pdf)
5. [http://www.opennetinitiative.net/studies/saudi/ONI\\_Saudi\\_Arabia\\_Country\\_Study.pdf](http://www.opennetinitiative.net/studies/saudi/ONI_Saudi_Arabia_Country_Study.pdf)
6. [http://www.opennetinitiative.net/studies/uae/ONI\\_UAE\\_Country\\_Study.pdf](http://www.opennetinitiative.net/studies/uae/ONI_UAE_Country_Study.pdf)
7. [http://www.opennetinitiative.net/studies/bahrain/ONI\\_Bahrain\\_Country\\_Study.pdf](http://www.opennetinitiative.net/studies/bahrain/ONI_Bahrain_Country_Study.pdf)
8. [http://www.opennetinitiative.net/studies/iran/ONI\\_Country\\_Study\\_Iran.pdf](http://www.opennetinitiative.net/studies/iran/ONI_Country_Study_Iran.pdf)
9. [http://www.opennetinitiative.net/studies/singapore/ONI\\_Cou](http://www.opennetinitiative.net/studies/singapore/ONI_Cou)

[ntry\\_Study\\_Singapore.pdf](#)

10.

[http://www.opennetinitiative.net/studies/burma/ONI\\_Burma\\_Country\\_Study.pdf](http://www.opennetinitiative.net/studies/burma/ONI_Burma_Country_Study.pdf)

11.

[http://www.opennetinitiative.net/studies/tunisia/ONI\\_Tunisia\\_Country\\_Study.pdf](http://www.opennetinitiative.net/studies/tunisia/ONI_Tunisia_Country_Study.pdf)

12. <http://anonymous-p2p.org/>

13.

<http://www.wired.com/news/politics/0,1283,17538,00.html>

14. <http://cryptome.org/>

15.

[http://www.astalavista.com/media/archive1/newsletter/issue\\_18\\_2005.pdf](http://www.astalavista.com/media/archive1/newsletter/issue_18_2005.pdf)

16. [http://reviews-zdnet.com.com/4520-7298\\_16-4207926.html](http://reviews-zdnet.com.com/4520-7298_16-4207926.html)

17. [http://www.cl.cam.ac.uk/~rnc1/Patterns\\_of\\_Failure.pdf](http://www.cl.cam.ac.uk/~rnc1/Patterns_of_Failure.pdf)

18. <http://homes.esat.kuleuven.be/~gdanezis/thesis.pdf>

19. <http://p3pbook.com/ch01.pdf>

20. <http://www.zensur.freerk.com/>

21. <http://www->

[users.cs.york.ac.uk/~susan/bib/ss/security/389.pdf](http://users.cs.york.ac.uk/~susan/bib/ss/security/389.pdf)

22. <http://www.securityfocus.com/columnists/356>

23.

<http://www2.norwich.edu/mkabay/overviews/anonpseudo.pdf>

24. <http://technorati.com/tag/privacy>

25. <http://technorati.com/tag/anonymity>

26. <http://technorati.com/tag/censorship>

27. <http://technorati.com/tag/free+speech>

28. <http://technorati.com/tag/digital+rights>

63

### **What are botnet herds up to? (2006-01-17 17:48)**

[1]Johannes B. Ullrich, with whom I had a [2]chat once, did a great [3]post providing us with real-life botnet herds

"know how" or the lack of such. And while I agree that these are newbies, they are exploiting another growing trend.

The vertical markers Johannes mentions are the result of abusing the affiliate networks themselves.

Though, how can an affiliate network distinguish traffic coming from botnets, should it count it as malicious one, can

they somehow link everything and see the entire picture? They sure can, but as soon as revenues keep coming in,

they simply wouldn't.

The botmasters' mentioned here are primarily acting as [4]domainers, and the possibilities for abuse here are count-

less. In case you're interested in knowing more about the use and abuse of such networks, I recommend you to go

through [5]Ben Edelman's research on [6]affiliate networks, and how [7]easily they get [8]abused. My point is that, if

it takes a newbie to start realizing this, imagine the big players, as there are obviously [9]some, at least in respect to the sizes of their botnets :)

If they make a buck for selling access to their resources, still have the opportunity to do it on their own, and cash again while giving instructions on how to "reinfect" yourself, that's a Ecosystem that I mentioned in my recently released

"[10]Malware - Future Trends" research. I feel this particular botnet herd is up to experiments, that obviously didn't go unnoticed.

What are your thoughts on the future of botnets, how would they abuse their power in [11]Web 2.0? Week

before I release my original publication, someone started coming up with "solutions" on how to abuse [12]Google's AdSense, there's a lot to come for sure!

In case you want to know more about botnets, consider going through the following :

[13]Bots and Botnets: Risks, Issues and Prevention

[14]The Zombie Roundup: Understanding, Detecting, and Disrupting Botnets

[15]Botnets as a Vehicle for Online Crime

[16]Botnets - the threat to the Critical National Infrastructure

[17]Botnet Detection and Response

[18]Tracking Botnets

[19]Robot Wars – How Botnets Work

[20]Worms, Viruses and Botnets - security awareness video

Technorati tags :

[21]malware,[22]security,[23]information security,  
[24]botnets

1. <http://johannes.homepc.org/>

2. [http://www.astalavista.com/media/archive1/newsletter/issue\\_21\\_2005.pdf](http://www.astalavista.com/media/archive1/newsletter/issue_21_2005.pdf)

3. <http://isc.sans.org/diary.php?date=2006-01-14>

4. <http://en.wikipedia.org/wiki/Domainer>

5. <http://www.benedelman.org/>

6. <http://www.benedelman.org/news/052305-1.html>

7. <http://www.benedelman.org/news/121905-1.html>

8. <http://www.benedelman.org/news/091405-1.html>

9. <http://www.vnunet.com/vnunet/news/2144375/botnet-operation-ruled-million>

10. [http://ddanchev.blogspot.com/2006/01/future-trends-of-malware\\_16.html](http://ddanchev.blogspot.com/2006/01/future-trends-of-malware_16.html)

11. <http://www.web2con.com/>

12. <http://www.techshout.com/internet/2005/27/a-trojan-horse-program-that-targets-google-ads-has-been-detected-by-an-indian-web-publisher/>

64

13. [http://arachnid.homeip.net/papers/VB2005-Bots\\_and\\_Botnets-1.0.2.pdf](http://arachnid.homeip.net/papers/VB2005-Bots_and_Botnets-1.0.2.pdf)

14. [http://www.arbornetworks.com/downloads/research130/sruti05\\_final.pdf](http://www.arbornetworks.com/downloads/research130/sruti05_final.pdf)

15. <http://www.cert.org/archive/pdf/Botnets.pdf>

16. [http://www.niscc.gov.uk/niscc/docs/botnet\\_11a.pdf](http://www.niscc.gov.uk/niscc/docs/botnet_11a.pdf)

17. <http://www.caida.org/projects/oarc/200507/slides/oarc0507-Dagon.pdf>

18. <http://www.honeynet.org/papers/bots/>

19. <http://www.windowsecurity.com/articles/Robot-Wars-How-Botnets-Work.html>

20. [http://www.waarschuwingsdienst.nl/movies/botnetfilm\\_en.wmv](http://www.waarschuwingsdienst.nl/movies/botnetfilm_en.wmv)

21. <http://technorati.com/tag/malware>

22. <http://technorati.com/tag/security>

23. <http://technorati.com/tag/information+security>

24. <http://technorati.com/tag/botnets>

65

### **China - the biggest black spot on the Internet's map (2006-01-17 17:49)**

Chinese Internet users have the potential to [1]outpace the number of the U.S Internet population, yet, the majority of them still remain behind the most sophisticated online censorship systems in the world, the [2]Great Chinese Firewall.

I am definitely not buying into the idea of trying to take control of all the information coming in and going out of a country for the sake of my well being, as any individual has the right to decide what's good and bad for them.

If I, for instance [3]knew there's a [4]virus on the streets of my city, I would take immediate precautions, or at least, see how "my" government reacts on the crisis. Yet, how responsible, moral, or legal according to international human rights standards is to prosecute users who have been spreading the news about the SARS virus from within the Great

Firewall is perhaps another point.

Isn't [5]central planning the panacea of Communism, be it, old-school or modern(an excuse for the old-school) one,



and isn't the obvious fact that the government cannot, but wants to play God, an utopia by itself? It is disturbing

how business ethics surpass moral ones for the sake of business continuity, so to say. Though, [6]efforts are made to

break the ice, until a collective campaign is not started I doubt anything will change. For the time being, what they

[7]don't like, they either hijack(forward to another site), or [8]completely restrict.

With over [9]100,000 cybercafes, and 30,000 state police enforcing policies on the Internet, the Chinese government

is trying to establish a very effective self-censorship atmosphere, namely, prosecuting those somehow violating it.

The idea is to, of course, cut the costs of their censorship efforts.

U.S companies don't have a [10]business choice, but to [11]comply in case they are interested in taking advantages of the business opportunities in the country.

[12]Activists have been expressing their attitude towards assistance like that, while I feel the majority of business

leaders still don't have the incentive to take action, besides the human moral obligations, ones that are often

neglected when doing business. [13]Sad, but true :)

For me, it's not businesses complying with local laws that bothers me, but the playground for the these vendors

that's fuelling innovation in the wrong direction. That very same innovation is later on to used on Western countries

or pretty much anywhere around the world. For the time being, [14]China is still winning against the Web, and the

term cyberdissident is getting rather common. For instance, the recently started [15]Cryptome.cn, pointed out a

great link to the actual known number of Chinese actions against [16]journalists. That's disturbing.

One of the most resourceful and timely research currently available is [17]ONI's [18]Internet Filtering in China in

2004-2005 : A Country Study. Interested in finding out whether a certain sites is currently blocked in China? Check

the [19]Real-Time Testing of Internet Filtering in China, courtesy of [20]Harvard Law School, whose [21]Empirical

Analysis of Internet Filtering in China still gives an overview of the situation and what's to consider.

Further research and opinions on the topic can be found at :

[22]Internet Development and Information Control in the People's Republic of China

[23]Internet censorship in mainland China

[24]The Internet in China: Civilian and Military Uses

[25]Internet in China: Big Mama is Watching You

[26]Internet Filtering in China

[27]The limits of Internet filtering : A moral case for the maximization of information access over the Internet

[28]Controlling Online Information: Censorship & Cultural Protection

[29]Tools for Censorship Resistance

[30]The Filtering Matrix

66

[31]Tor: An anonymous Internet communication system

Technorati tags :

[32]privacy,[33]free speech,[34]china censorship,[35]china,[36]censorship

1.

<http://www.technewsworld.com/story/6GWreZVU0CpkDv/Report-China-Internet-Use-Catching-Up-With-US.xhtml>

2. [http://en.wikipedia.org/wiki/Great\\_Firewall](http://en.wikipedia.org/wiki/Great_Firewall)

3. <http://www.hrichina.org/public/contents/9004>

4.

<http://edition.cnn.com/2003/WORLD/asiapcf/east/05/14/sars.censor/index.html>

5. [http://en.wikipedia.org/wiki/Planned\\_economy](http://en.wikipedia.org/wiki/Planned_economy)

6. [http://www.financialmirror.com/more\\_news.php?id=2973](http://www.financialmirror.com/more_news.php?id=2973)

7. <http://news.bbc.co.uk/1/hi/technology/4056255.stm>

8. [http://www.theregister.co.uk/2002/09/02/china\\_blocks\\_google\\_allegedly/](http://www.theregister.co.uk/2002/09/02/china_blocks_google_allegedly/)
9. <http://news.bbc.co.uk/2/hi/technology/3699820.stm>
10. [http://www.forbes.com/2006/01/04/gates-microsoft-china-cx\\_cn\\_0104autofacescan09.html](http://www.forbes.com/2006/01/04/gates-microsoft-china-cx_cn_0104autofacescan09.html)
11. <http://news.bbc.co.uk/1/hi/world/asia-pacific/4221538.stm>
12. <http://cryptome.org/yahoo-rats.htm>
13. <http://www.sing365.com/music/lyric.nsf/Sad-But-True-lyrics-Metallica/DB6271E5103CDD284825688D0033DF75>
14. <http://www.nytimes.com/2006/01/15/weekinreview/15zeller.html>
15. <http://www.cryptome.cn/>
16. [http://www.cpj.org/regions\\_06/asia\\_06/asia\\_06.html#china](http://www.cpj.org/regions_06/asia_06/asia_06.html#china)
17. <https://web.archive.org/web/20101016193525/http://www.opennetinitiative.net/>
18. [http://www.opennetinitiative.net/studies/china/ONI\\_China\\_Country\\_Study.pdf](http://www.opennetinitiative.net/studies/china/ONI_China_Country_Study.pdf)
19. <http://cyber.law.harvard.edu/filtering/china/test/>
20. <http://www.law.harvard.edu/>

21. <http://cyber.law.harvard.edu/filtering/china/>
22. <http://www.fas.org/sgp/crs/row/RL33167.pdf>
23. [http://en.wikipedia.org/wiki/Internet\\_censorship\\_in\\_China](http://en.wikipedia.org/wiki/Internet_censorship_in_China)
24. <http://fmso.leavenworth.army.mil/documents/china-internet.htm>
25. <http://www.lokman.nu/thesis/010717-thesis.pdf>
26. <http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan011043.pdf>
27. <http://www.everythingispolitical.ca/journal/essay12.pdf>
28. [http://www.kus.uu.se/pdf/publications/ICT/klang\\_03\\_oct.pdf](http://www.kus.uu.se/pdf/publications/ICT/klang_03_oct.pdf)
29. <http://www.eecs.harvard.edu/~greenie/defcon-slides.pdf>
30. <http://ice.citizenlab.org/ppt/FilteringMatrix-4.0.pdf>
31. <http://tor.eff.org/>
32. <http://technorati.com/tag/privacy>
33. <http://technorati.com/tag/free+speech>
34. <http://technorati.com/tag/china+censorship>
35. <http://technorati.com/tag/china>
36. <https://web.archive.org/web/20101016193525/http://technorati.com/tag/censorship>

## **FBI's 2005 Computer Crime Survey - what's to consider? (2006-01-19 17:51)**

Yesterday, the FBI has [1]released their [2]Annual 2005 Computer Crime Survey, and while I bet many other comments

will also follow, I have decided to comment on it the way I've been [3]commenting on the U.S 2004's "[4]Annual Report to Congress on Foreign Economic Collection and Industrial Espionage" in previous posts. This one is compiled based

on the 24, 000 participating organizations from 430 cities within the U.S, so look for the averages where possible :)

What are the key summary points, and what you should keep in mind?

### **- Attacks are on the rise, as always**

That's greatly anticipated given the ever growing Internet penetration and the number of new users whose

bandwidth power is reaching levels of a middle sized ISP. Taking into consideration the corporate migration towards

IP based business infrastructure, and even the [5]military's interest in that, it results in quite a lot of both,

visible/invisible targets. My point is that, to a certain extend a new Internet user is exposed to a variety of events

that are always static in terms of security breaches, or was it like that several years ago? Less [6]0day's, lack of client

side vulnerabilities([7]browsers) the way we are seeing it today, and cookies compared to [8]spyware were the

"worst" that could happen to you. Things have changed, but malware is still on the top of every survey/research you would come across.

### **- The threat from within**

[9]Insiders dominate the corporate threatscape as always, and the average financial losses due to

"Laptop/Desktop/PDA Theft", act as an indicator for intellectual or sensitive property theft that is actively quantified to a certain extent, though it is still mentioned in a separate section. As far as insiders and the responses given in

here, " *the threat you're currently not aware of, is the threat actually happening*" to quote a McAfee's ad I recently came across to. Especially in respect to insiders.

### **- [10]To report or not to report?**

*According to the survey " Just 9 % said they reported incidents to law enforcement, believing the infractions were not illegal or that there was little law enforcement could or would do. Of those reporting, however, 91 % were satisfied with law enforcement's response. And 81 % said they'd report future incidents to the FBI or other law enforcement agencies."*

The key point here is the lack of understanding of what a threat is, or perhaps what exactly should be reported, or

why bother at all? And given that out of the 9 % reporting 91 % are satisfied I can simply say that, " *If you don't take care of your destiny, someone else will*".

Overall, you should consider that the lack of quality statistics is the result of both, the "stick to the big picture"

research and survey approaches, or because of companies not interested/understanding what a security threat

worth reporting actually is? I greatly feel the industry and the Internet as a whole is in need of a commonly accepted

approach, and while such exist, [11]someone [12]has [13]to perhaps communicate them in a more effective way.

Broad and unstructured definitions of security, result in a great deal of insecurities to a certain extend, or have the

potential to, doesn't they?

### **- Who's attacking them?**

Their homeland's infrastructure and the Chinese one, as the top attacks originally came from " *The U.S. (26.1 %) and China (23.9 %) were the source of over half of the intrusion attempts, though masking technologies make it difficult* 68

*to get an accurate reading*", and yes, Russia "of course".

Though, you should keep in mind that whenever someone sparkles a debate on certain country's netblocks attacking another country's one, it's always [14]questionable.

### **- What measures are actually taken?**



Besides actively investing in further solutions, and re-evaluating their current measures, what made me an

impression as worth mentioning is :

- **patching**, whether the patch comes from a [15]third-party or the vendor itself is something else, yes it's the

reactive measure that could indeed eliminate "known" vulnerabilities, yet it's proactive approaches companies

should aim at achieving

- **keeping it quiet**, as you can see the 3rd measure taken is to actually not report what has happened, wrong, both in respect to the actual state of security, and the potential consequences in case a sensitive info breach occurred and

customers did the job of reporting and linking it.

- **tracing back?** I think it's a bit unrealistic in today's botnets dominated Internet, namely an enterprise might find out that some of its external port scans are coming from internal infected PCs. When attacked you always want to know

where the hell is it coming from, and who's involved, and while entirely based on the attackers techniques put in

place, I feel that close cooperation with ISPs in reporting the infected nodes should get the priority compared to

tracing the attacks back. That greatly depends on the attack, its severity, and traceability of course.

To sum up, the bottom line is that, [16]antivirus software and [17]perimeter based defenses dominate the

perception of security as always, companies are actively investing in security and would continue to do so. It's a very recent [18]survey for you to use, or brainstorm on!

Technorati tags :

[19]security,[20]information security,[21]security statistics,  
[22]security trends,[23]FBI

1.  
[http://www.fbi.gov/page2/jan06/computer\\_crime\\_survey011806.htm](http://www.fbi.gov/page2/jan06/computer_crime_survey011806.htm)
2.  
<http://www.cpppe.umd.edu/Bookstore/Documents/2005CSISurvey.pdf>
3. <http://ddanchev.blogspot.com/2005/12/insiders-insights-trends-and-possible.html>
4.  
[http://www.nacic.gov/publications/reports\\_speeches/reports/fecie\\_all/fecie\\_2004/FecieAnnual%20report\\_2004\\_NoCoverPages.pdf](http://www.nacic.gov/publications/reports_speeches/reports/fecie_all/fecie_2004/FecieAnnual%20report_2004_NoCoverPages.pdf)
5. <http://www.fas.org/man/crs/RL32411.pdf>
6. <http://ddanchev.blogspot.com/2005/12/0bay-how-realistic-is-market-for.html>
7. <http://bcheck.scanit.be/bcheck/page.php?name=STATS2004>
8.  
<https://web.archive.org/web/20101016193525/http://www.pywareinfo.com/>

9. <http://ddanchev.blogspot.com/2005/12/insiders-insights-trends-and-possible.html>
10. <http://ddanchev.blogspot.com/2006/01/to-report-or-not-to-report.html>
11. <http://www.fbi.gov/>
12. <http://www.secretservice.gov/>
13. <http://www.cert.org/>
14. <https://draft.blogger.com/http://ddanchev.blogspot.com/2005/12/ip-cloaking-and-competitive.html>
15. <http://www.securityfocus.com/columnists/378>
16. <https://draft.blogger.com/http://www.viruslist.com/en/analyses?pubid=174405517>
17. <http://www.csoononline.com/read/110105/machine.html>
18. <http://www.fbi.gov/publications/ccs2005.pdf>
- 69
19. <http://technorati.com/tag/security>
20. <http://technorati.com/tag/information+security>
21. <http://technorati.com/tag/security+statistics>
22. <http://technorati.com/tag/security+trends>
23. <http://technorati.com/tag/FBI>

## **Why relying on virus signatures simply doesn't work anymore? (2006-01-19 17:52)**

As a fan of [1]VirusTotal and [2]Norman's Sandbox being always handy when making analyses or conclusions, and me looking for metrics and data to base my judgments on, besides experience, I feel their "Failures in Detection" of VT deserve more attention than they're actually getting.

With over 14,000 files submitted on a weekly basis, where most of them are supposedly 0day malicious software,

it's a great resource to consider. Using [3]these scanners for the basis of its service (saw yours?!), it is still able to conclude the plain truth - signature based anti virus protection is having deep troubles as a concept these days.

Moreover, vendors covering or enjoying monopolistic competition in specific geographical regions, without having the necessary AV expertise is something that is actually happening. So what made me an [4]impression?

### **Failures in Detection (Last 7 days)**

- **14,016 failures** that is, infected files not detected by at least one antivirus engine

- **372 samples detected** by all vendors

What's important to note here is that, response time towards a new piece of malware in the wild is crucial as always.

But that's great when it's actually achieved. The independent folks at [5]Av-test.org, have featured a very nice Excel

sheet on the "[6]Reaction Times of the latest MS05-039-based Worm Attacks"(2005-08-22) so you can take a look for yourself.

And as I've once mentioned my opinion on the growing possibility of [7]0day malware on demand, proactive

measures would hopefully get the attention of vendors. Some folks are going as high as stating that AV scanners and

AV defense as a concept will eventually end up as product line extension of a security appliance? Though, I feel you

will never be able to license a core competency of a vendor that's been there before the concept of DDoS started

getting public! And obviously, the number of signatures detected by them doesn't play a major role like it used years

ago. Today's competitive factors have to do with, but not only of course :

**Heuristic**

**Policy-Based Security**

**IPS (Intrusion Prevention Systems)**

**Behaviour Blockers**

**Protection against Buffer Overruns**

I also advise you to go through a well written research on the topic of [8]Proactive Antivirus protection, as it

highlights the issues to keep in mind in respect to each of these. Is client side sandboxing an [9]alternative as well,

could and would a customer agree to act as a sandbox compared to the current(if any!) contribution of forwarding a

suspicious sample? Would v2.0 constitute of a [10]collective automated web patrol in a PC's "spare time"? How

sound is this and the other concepts in terms of usability and deployment on a large scale?

Signatures are always a necessary evil as I like to say, ensure that at least your anti virus software vendor is not a

newly born company with a modest honeyfarm and starting to perceive itself as a vendor, vendor of what? Solutions

or signatures?!

Don't get me wrong, my intention behind this post was to make you think, as a customer or decision-maker on the

approaches your current vendor uses, and how to make better decisions. At the bottom line, it's still a vendor's

sensor network or client side submissions, even exchange of data between them, that provides the fastest response

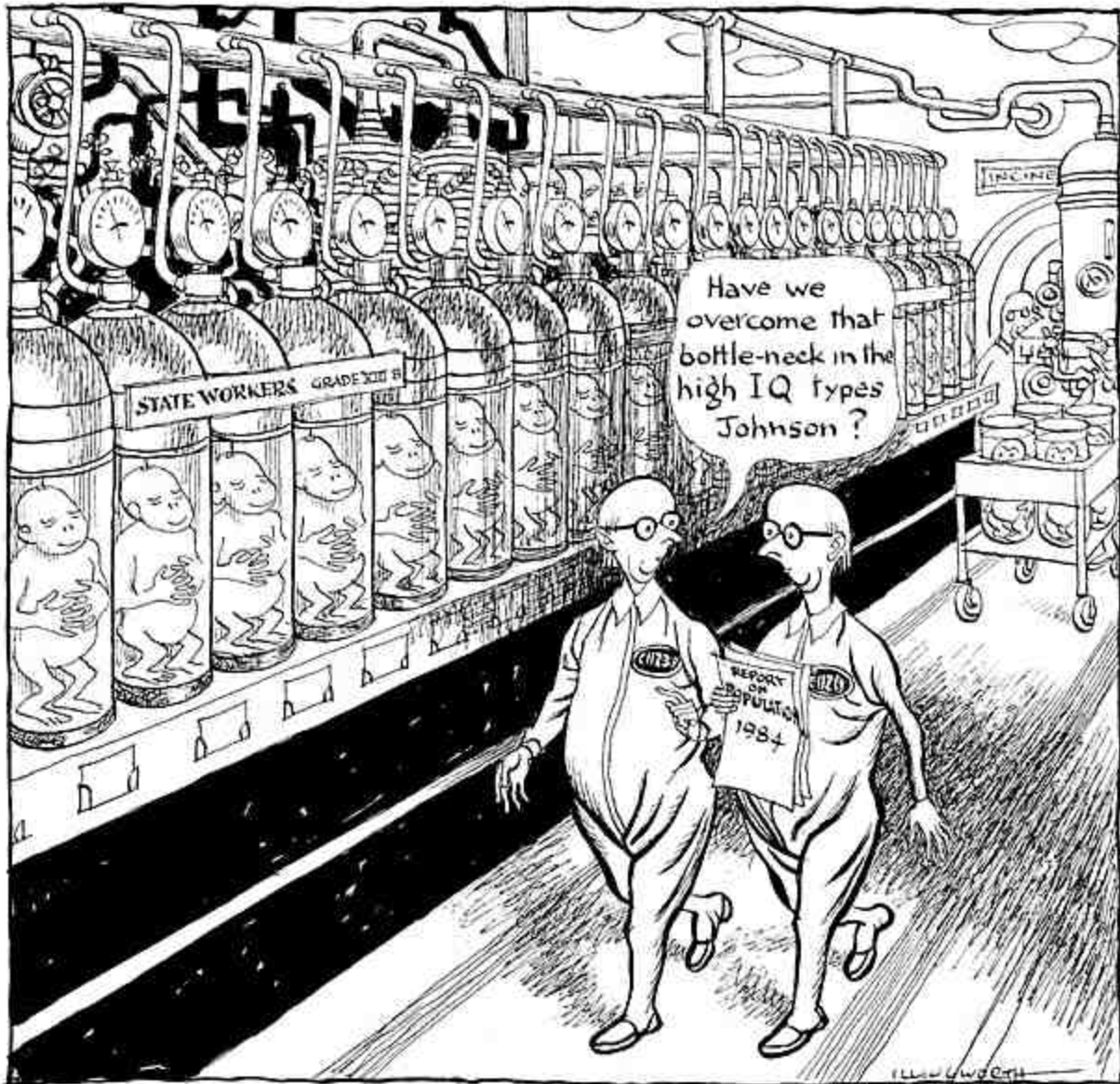
to \*known\* malware!

71

Technorati tags :

[11]security,[12]information security,[13]malware,  
[14]viruses,[15]antivirus,[16]malware trends

1. <http://www.virustotal.com/>
2. <http://sandbox.norman.no/>
3. [http://www.virustotal.com/flash/virustotal\\_en.html](http://www.virustotal.com/flash/virustotal_en.html)
4. [http://www.virustotal.com/flash/estadisticas\\_en.html](http://www.virustotal.com/flash/estadisticas_en.html)
5. <http://www.av-test.org/>
6. <http://www.av-test.org/download/ms05-039.zip>
7. <http://www.packetstormsecurity.org/papers/general/malware-trends.pdf>
8. [http://www.viruslist.com/en/downloads/vlpdfs/wp\\_nikishin\\_proactive\\_en.pdf](http://www.viruslist.com/en/downloads/vlpdfs/wp_nikishin_proactive_en.pdf)
9. <http://www.vmware.com/vmtn/vm/browserapp.html>
10. <http://research.microsoft.com/honeymonkey/>
11. <http://technorati.com/tag/security>
12. <http://technorati.com/tag/information+security>
13. <http://technorati.com/tag/malware>
14. <http://technorati.com/tag/viruses>
15. <http://technorati.com/tag/antivirus>
16. <http://technorati.com/tag/malware+trends>



**2006 = 1984? (2006-01-23 17:54)**

[1]

I recently came across great, and very informative slides on current, and future trends of surveillance technologies



that simply stick to the point, as any good slides so to say. "[2]From Target Market to Total Surveillance" is courtesy of the [3]The Special Interest Group for Military Applications (SIGMil) at the University of Illinois, and is among the many [4]talks and quality [5]projects they have running.

" *The Survey of Orwellian Technologies*" outlines the current situation of privacy invasion and who's who on the market for censorship solutions.

For instance it correctly states that :

- **[6]Cisco** built the Great Firewall at discount to corner router market

73

-Video and telephone surveillance networks

-Buying habits and physical location history

-Net access history, web posts and email

**[7]Nortel**, developed network traffic analysis system dedicated to catching political opposition (Falun Gong)

**Motorola**, competed with Nokia to provide location tracking

**Microsoft**, [8]censors words in blog software

**[9]Yahoo**, actively collaborates in tracking state political opponents via their email, search and chat usage

**Google**, censors prohibited sites/queries from search- Alters news results to favor nationalized news(Still, Google recently [10]declined the request for access for its

databases, compared to the rest of search engines, Yahoo!, MSN)

The worst in this case, from my point of view the experience gained by the companies, in the wrong direction.

I once [11]mentioned how businesses don't have a business choice but to comply, the thing is now the Western

media has already started [12]seeking accountability and higher levels of moral.

Basically, profitability shouldn't be an objective, when encouraging the further development of such "regimes". I guess, I still don't have a content filtering agreement with the Chinese government, but I don't even want to...:)

The entire idea of censorship in here is to avoid events in direct confrontation with current "reality", and I think the it isn't wise, [13]keeping it quiet is even worse. The bad thing is that even IBM used to do [14]"business" with the wrong party I guess . What is greed and profit maximization, what is business and morale? Words we remember on

Xmas's day for sure!

More info on the topic can also be found at :

[15]International Campaign Against Mass Surveillance

[16]Balancing surveillance

74

[17]Justifying the cost of digital video surveillance

[18]Protecting Personal Data in Camera Surveillance

[19]Society-and-Surveillance study journal

Technorati tags :

[20]security,[21]privacy,[22]free speech,[23]censorship,  
[24]surveillance,[25]1984

1.  
<https://photos1.blogger.com/blogger/1933/1779/1600/ilw1611.gif>
2. <http://www.acm.uiuc.edu/sigmil/talks/Orwellian.pdf>
3. <http://www.acm.uiuc.edu/sigmil/index.shtml>
4. <http://www.acm.uiuc.edu/sigmil/talks.shtml>
5. <http://www.acm.uiuc.edu/sigmil/projects.shtml>
6. <http://yaleglobal.yale.edu/display.article?id=5928>
7. [http://www.fofg.org/news/news\\_story.php?doc\\_id=815](http://www.fofg.org/news/news_story.php?doc_id=815)
8. <http://www.asiamedia.ucla.edu/article.asp?parentid=37346>
9.  
[https://web.archive.org/web/20101016193525/http://www.usatoday.com/news/opinion/editorials/2005-06-19-our-view\\_x.htm](https://web.archive.org/web/20101016193525/http://www.usatoday.com/news/opinion/editorials/2005-06-19-our-view_x.htm)
10. <http://blog.searchenginewatch.com/blog/060119-060352>
11. <http://ddanchev.blogspot.com/2006/01/china-biggest-black-spot-on-internets.html>

12. <http://www.axcessnews.com/modules/wfsection/article.php?articleid=7607>
13. [http://www.financialmirror.com/more\\_news.php?id=2973](http://www.financialmirror.com/more_news.php?id=2973)
14. <http://news.com.com/2009-1082-269157.html>
15. <http://www.i-cams.org/ICAMS1.pdf>
16. <http://www.securityfocus.com/columnists/366>
17. [http://www.csoononline.com/read/090105/roi\\_3826.html](http://www.csoononline.com/read/090105/roi_3826.html)
18. <http://www.surveillance-and-society.org/articles2%284%29/protecting.pdf>
19. <http://www.surveillance-and-society.org/>
20. <http://technorati.com/tag/security>
21. <http://technorati.com/tag/privacy>
22. <http://technorati.com/tag/free+speech>
23. <http://technorati.com/tag/censorship>
24. <http://technorati.com/tag/surveillance>
25. <http://technorati.com/tag/1984>

75

## **Cyberterrorism - recent developments (2006-01-23 17:57)**

I've once blogged about why you shouldn't [1]stereotype when it comes to Cyberterrorism, and going through the

most recent and well researched report on "[2]Terrorism Capabilities for Cyberattack : Overview and Policy Issues" I came across great similarities to what I posted. I think cyberterrorism shouldn't be just perceived as shutting down a

stock exchange, or slowing it down, the irony here is that it could actually [3]happen for "good" on a certain occasions

:)

Going back to the report, it's a very recent overview of cyberterrorism, and the way it's perceived. Flawed or not I'll

leave up to you to decide. What made me an impression anyway?

- [4]CIA's 2005 "Silent Horizon" to practice defending against a simulated widespread cyberattack directed against the United States. I really don't think frontal attack are of any interest, or are they?

- [5]Stolen credit cards were used in the terrorist attacks in Bali. There have also been other [6]cases, of exactly the same, using cyber activities for funding real world crime and terrorism.

- How [7]sensitive information on a future Army command and control system was stolen from an unclassified

system by at least [8]reportedly, Chinese hackers. Unclassified doesn't necessarily mean someone wasn't having a

false sense of security on a .mil domain I guess.

- The [9]U.S Elite Military Hacking Crew, the so called Joint Functional Component Command for Network Warfare

(JFCCNW) I feel every military forces have or should have these.

The report also highlights that the Internet is now a [10]prime recruiting tool for insurgents in Iraq. Insurgents have

created many Arabic-language Web sites that are said to contain coded plans for new attacks. Some reportedly give

advice on how to build and operate weapons, and how to pass through border checkpoints .

- Other news articles report that a [11]younger generation of terrorists and extremists, such as those behind the July

2005 bombings in London, are learning new technical skills to help them avoid detection by law enforcement

computer technology

Which is exactly what I've mentioned in my post on [12]Cyberterrorism. I feel, communication, and coordination,

besides [13]research is the ultimate goal here.

The only thing that make made me sort of a bad impression was how the only major innovation mentioned is

[14]quantum cryptography, and [15]steganography mentioned just twice. I think that this isn't entirely the case, and

breaking cryptography doesn't necessarily have to come in form of directly attacking the algorithm itself. That

happens to be impossible sometimes, but the first time when I came across the fact that the AU [16]government can

use spyware on criminals with the idea too obtain keys, or whatsoever, it makes such [17]issues irrelevant.

On the other hand, the way the Internet provides "them" with more opportunities, the more their [18]traceability

[19]improves, or at least give clues to a certain extend.

Technorati tags :

[20]security,[21]information security,[22]cyberterrorism,  
[23]Terrorism,[24]al qaeda

1. <http://ddanchev.blogspot.com/2005/12/cyberterrorism-dont-stereotype-and-its.html>

2. <http://www.opencrs.com/document/RL33123/>

3.  
<http://edition.cnn.com/2006/BUSINESS/01/19/tse.changes.reut/>

4.  
<http://www.wired.com/news/politics/0,1283,67644,00.html?tw=rss.TOP>

76

5.  
<http://www.lasvegassun.com/sunbin/stories/text/2005/apr/13/518595803.html>

6. <http://www.securityfocus.com/brief/42>

7. <http://www.time.com/time/nation/printout/0,8816,1098371,00.html>
8. <http://ddanchev.blogspot.com/2005/12/ip-cloaking-and-competitive.html>
9. <http://www.wired.com/news/privacy/1,67223-0.html>
10. <http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2005/07/10/CURIEL.TMP>
11. <http://www.timesonline.co.uk/article/0,,22989-1690459,00.html>
12. <http://ddanchev.blogspot.com/2005/12/cyberterrorism-dont-stereotype-and-its.html>
13. [http://en.wikipedia.org/wiki/Open\\_source\\_intelligence](http://en.wikipedia.org/wiki/Open_source_intelligence)
14. [http://en.wikipedia.org/wiki/Quantum\\_cryptography](http://en.wikipedia.org/wiki/Quantum_cryptography)
15. <http://en.wikipedia.org/wiki/Steganography>
16. <http://it.slashdot.org/article.pl?sid=04/12/13/1925240&tid=172&tid=17>
17. <http://www.techworld.com/news/index.cfm?newsID=4727&printerfriendly=1>
18. [http://www.cl.cam.ac.uk/~rnc1/The\\_Limits\\_of\\_Traceability.html](http://www.cl.cam.ac.uk/~rnc1/The_Limits_of_Traceability.html)
19. <http://www.cse.ucsd.edu/users/tkohno/papers/PDF/KoBrCl05PDF-lowres.pdf>



20. <http://technorati.com/tag/security>
21. <http://technorati.com/tag/information+security>
22. <http://technorati.com/tag/cyberterrorism>
23. <http://technorati.com/tag/Terrorism>
24. <http://technorati.com/tag/al+qaeda>

77



## **Still worry about your search history and BigBrother? (2006-01-23 17:59)**

[1]

[2]The Patriot Search, recently started "helping" any government by making your

search activity "public". Its search syntax *terrorist:true \*keyword\**, and *terrorist:false \*keyword\**, gives everyone the opportunity to be honest :) Why did the idea start at the [3]first place?

Because "[4]only 4 out of 5 search engines allowed the government to see "private" user data". Though, a distinction between [5]private searches VS personally identifiable searches should be made as well.

What's going to happen in the future? [6]Search engines regulation, [7]P3P, or [8]stock market losses due to an

[9]initiative whose requirements I feel were totally wrong from the very beginning?

Consider going though [10]David Berlind's comments as well!

Technorati tags :

[11]google,[12]bush,[13]privacy,[14]search engine

1. [https://web.archive.org/web/20101016193525/http://photos1.blogger.com/blogger/1933/1779/1600/Patriot\\_Search\\_h.0.jpg](https://web.archive.org/web/20101016193525/http://photos1.blogger.com/blogger/1933/1779/1600/Patriot_Search_h.0.jpg)
2. <http://blog.outer-court.com/patriot/>
3. [http://www.mercurynews.com/mld/mercurynews/news/breaking\\_news/13682492.htm](http://www.mercurynews.com/mld/mercurynews/news/breaking_news/13682492.htm)
4. <http://blog.outer-court.com/archive/2006-01-19-n45.html>
5. <https://web.archive.org/web/20101016193525/http://blog.searchenginewatch.com/blog/060123-074811>
6. <http://islandia.law.yale.edu/isp/regulatingsearch.html>
7. <http://www.p3ptoolbox.org/>
8. [http://money.cnn.com/2006/01/20/technology/google\\_stock/index.htm](http://money.cnn.com/2006/01/20/technology/google_stock/index.htm)
9. <http://www.usdoj.gov/osg/briefs/2003/3mer/2mer/2003-0218.mer.aa.html>

10. <http://blogs.zdnet.com/BTL/?p=2454>
11. <http://technorati.com/tag/google>
12. <http://technorati.com/tag/bush>
13. <http://technorati.com/tag/privacy>
14. <http://technorati.com/tag/search+engine>

78



## **Homebrew Hacking, bring your Nintendo DS! (2006-01-23 18:00)**

[1]

Yesterday, Engadget [2]reported about a "WiFi sniffer" that turns your [3]Nin-

tendo DS, into a wardriving tool and while it lacks certain features, it can still prove "handy", even fuel further security concerns over this [4]steadily [5]developing [6]trend [7]of homebrew hacking experiments.

[8]Removable media is a problem, but would gaming devices turn into a security threat as well? They can sure result

in more [9]malware, and this [10]trend, among the many other, made me an impression in respect to the need of

[11]interoperability in the upcoming future.

Technorati tags :

[12]security,[13]information security,[14]hacking,  
[15]homebrew,[16]nintendo,[17]nintendo DS

1. <https://web.archive.org/web/20101016193525/http://photos1.blogger.com/blogger/1933/1779/1600/dswar.jpg>
2. <http://www.engadget.com/2006/01/22/wifi-sniffer-turns-your-ds-into-a-wardriving-tool/>
3. <http://www.nintendo.com/systemsds>
4. <http://www.hackaday.com/>
5. <http://www.bottledlight.com/ds/>
6. <http://darkfader.net/ds/>
7. <http://www.psp-hacks.com/>
8. <http://www.continuitycentral.com/feature0184.htm>
9. [http://www.f-secure.com/weblog/archives/bricking\\_psp.wmv](http://www.f-secure.com/weblog/archives/bricking_psp.wmv)
10. <http://packetstormsecurity.org/papers/general/malware-trends.pdf>
11. <http://en.wikipedia.org/wiki/Interoperability>
12. <http://technorati.com/tag/security>

13. <http://technorati.com/tag/information+security>.
14. <http://technorati.com/tag/hacking>
15. <http://technorati.com/tag/homebrew>
16. <http://technorati.com/tag/nintendo>
17. <http://technorati.com/tag/nintendo+DS>



Category:	General	Applied	Technical	Functional	System	Design
Model Type	Network	Network	Network	Network	Network	Network
Example	Network	Network	Network	Network	Network	Network



## Visualization, Intelligence and the Starlight project (2006-01-23 18:01)

[1]

Today, I came across a [2]stunning collection of complex networks visualizations,

that reminded of how we must first learn to visualize and then go deeper into [3]VR. Until, I first visited this [4]project, the [5]Atlas of Cyberspace was perhaps my favorite visualization resource, rather outdated, still has a lot to show.

Visualization is important for today's greatly developed knowledge networks, data mining, and even information secu-

city or basic network management issues. But at the bottom line, who always has the best toys, or at least develops

them? The academic world? Sort of, except that they need the private sector to go public, so that leaves the U.S

military in my point of view :) and they sure do.

[6]

[7]The Starlight - Information Visualization Technology is simply a remarkable concept that these [8]folks actually

turned into a reality. It uses both structured, unstructured, spatial and multimedia data and provides real-time

output, and if you also consider that the project is reportedly down several years ago, for me it opens up the

question, who's the successor?

[9]

It's [10]national security applications and the syndication of data sources are so

clearly visible, that reducing paper-work, platform dependence, [11]information sharing, and perhaps not another

[12]Able Danger scenario(if one actually [13]happened!) is the biggest advantage of such a project.

Going back to the "reality"(yeah sure!), in case you've never seen [14]ChicagoCrimes, the free database of crimes reported in Chicago, it's yet another great initiative that again visualizes based on reports and [15]Google Maps, and

you don't need a security clearance to use it :) What's else to mention, is CNET's introduction of "[16]The Big

Picture" in cooperation with [17]Liveplasma.com of course, clearly, the waves of information flow must be somehow

filtered and there's a clear, both, commercial, public and intelligence need for it. Even [18]VR [19]investments are

actively taking place, a lot's to come for sure!

Some concepts and clips on visualization :

[20]TouchGraph Google Browser

[21]Real-Time and Forensic Network Data Analysis Using Animated and Coordinated Visualization

[22]F-Secure's visualization of the 1st PC virus, and [23]W32.Bagle, and you can actually see the [24]clip itself.

[25]Visualization study the U.S - clip

Technoratai tags :

80

[26]security,[27]information security,[28]intelligence, [29]OSINT,[30]starlight,[31]visualization,[32]virtual reality 1.

[https://web.archive.org/web/20101016193525im\\_/http://photos1.blogger.com/blogger/1933/1779/200/starlight.jp](https://web.archive.org/web/20101016193525im_/http://photos1.blogger.com/blogger/1933/1779/200/starlight.jpg)

g

2. <http://www.visualcomplexity.com/vc/index.cfm>

3. [http://en.wikipedia.org/wiki/Virtual\\_reality](http://en.wikipedia.org/wiki/Virtual_reality)



4. <http://www.visualcomplexity.com/vc/about.html>
5. <http://www.cybergeography.org/atlas/atlas.html>
6. <https://web.archive.org/web/20101016193525/http://photos1.blogger.com/blogger/1933/1779/1600/oinfomodel.gif>
7. <http://starlight.pnl.gov/>
8. <http://starlight.pnl.gov/index.asp?src=team.stm>
9. <https://web.archive.org/web/20101016193525/http://photos1.blogger.com/blogger/1933/1779/1600/appMilitary1.gif>
10. <http://starlight.pnl.gov/appMilitary.stm>
11. [http://www.govexec.com/story\\_page.cfm?articleid=33191&dcn=todaysnews](http://www.govexec.com/story_page.cfm?articleid=33191&dcn=todaysnews)
12. [http://en.wikipedia.org/wiki/Able\\_Danger](http://en.wikipedia.org/wiki/Able_Danger)
13. [http://www.9-11pdp.org/press/2005-11-21\\_letter.pdf](http://www.9-11pdp.org/press/2005-11-21_letter.pdf)
14. <http://www.chicagocrime.org/>
15. <http://www.chicagocrime.org/map/>
16. [http://news.com.com/The+Big+Picture/2030-12\\_3-5843390.html?tag=st.bp](http://news.com.com/The+Big+Picture/2030-12_3-5843390.html?tag=st.bp)
17. <http://liveplasma.com/>
18. [http://www.digitalglobe.com/images/intersat\\_pr/](http://www.digitalglobe.com/images/intersat_pr/)

19. <http://www.prnewswire.com/cgi-bin/stories.pl?ACCT=104&STORY=/www/story/01-04-2006/0004242166&EDATE=>
20. <http://www.touchgraph.com/TGGoogleBrowser.html>
21. [http://www.ece.gatech.edu/research/labs/nsa/papers/drafts/iaw\\_vis\\_draft.pdf](http://www.ece.gatech.edu/research/labs/nsa/papers/drafts/iaw_vis_draft.pdf)
22. <http://www.f-secure.com/weblog/archives/brain-a-750.png>
23. [http://www.f-secure.com/weblog/archives/f-secure\\_bagle-ag\\_visualization.jpg](http://www.f-secure.com/weblog/archives/f-secure_bagle-ag_visualization.jpg)
24. [http://www.f-secure.com/weblog/archives/f-secure\\_bagle-ag\\_visualization.wmv](http://www.f-secure.com/weblog/archives/f-secure_bagle-ag_visualization.wmv)
25. <http://archive.ncsa.uiuc.edu/SCMS/DigLib/movies/Visualization-Study-NSFNET-Cox.5549.mpg>
26. <http://technorati.com/tag/security>
27. <http://technorati.com/tag/information+security>
28. <http://technorati.com/tag/intelligence>
29. <http://technorati.com/tag/OSINT>
30. <http://technorati.com/tag/starlight>
31. <http://technorati.com/tag/visualization>
32. <http://technorati.com/tag/virtual+reality>



## **The Feds, Google, MSN's reaction, and how you got "bigbrothered"? (2006-01-24 18:03)**

[1]

There's still a lot of buzz going on, concerning which [2]search engine provided

what type of data to law [3]enforcement officials, and the echo effect of this event resulted in waves of [4]angry end

users, that among feeling "bigbrothered", now have yet another reason to switch back to Google, simple. MSN's silent reaction to this is the worst thing they could do given how actively they're trying to catch-up on search traffic. What

did they provide anyway?

*"Specifically, we produced a random sample of pages from our index and some aggregated query logs that listed*

*queries and how often they occurred. Absolutely no personal data was involved. With this data you :*

*CAN see how frequently some query terms occurred*

*CANNOT look up an IP and see what they queried*

*CANNOT look for users who queried for both "TERM A" and "TERM B"*

So picture, the following, "someone" requests his name, his friends' names, physical locations giving clues on possible area and while it isn't personal information(exact names, address etc.) it is personally identifiable one! If it happens once, it would become a habit, my point is that aggregating search info on [5]ECHELON's wordlist is so

realistic that you need a company to say NO, and evaluate the reactions of the others. The best thing is that I'm sure

the majority of adult entertainment seekers don't need to take advantage of [6]Echelon's Trigger Words Generator :)

Why you don't need to issue a [7]subpoena to find out what's hot in the online porn world?

- take Google's [8]advice into consideration, or start using [9]Overture's keyword selector tool

- now ensure you have the most popular porn related keywords, and if in doubt, consult with an "insider" who would be definitely aware of what's hot, and who's to keep in mind

- use the first 20 pages from each popular search for your sample, these get the majority of traffic

- do a little research over [10]Alexa to further back up your statements, and even use Google to measure the relative

popularity of the first site that pop ups when you search for [11]porn.

- ensure you have first consulted with traffic aggregators or [12]paid reports on who's who online
- make sure before going online, another distribution vector so to say, [13]the iPod is taken care of
- envision [14]what's to come in the future, and mostly the interest and the social implications of these issues
- now, come up with ways to restrict children from using these going beyond the usual "But of course I'm over 21 years old" terms of use

[15]

What's to come up in the future? In one of my previous posts "[16]Still worry

about your search history and BigBrother?" I pointed out the possibilities for [17]Search engines regulation and

[18]P3P, but the current self regulation is simply not working anymore.

Further resources on the topic can be found at :

82

[19]Lorrie Cranor's [20]Searching for Privacy : Design and Implementation of a P3P-Enabled Search Engine

[21]PrivacyBird

[22]An Analysis of P3P-Enabled Web Sites among Top-20 Search Results

[23]Protecting Your Search Privacy: A Flowchart To Tracks You Leave Behind

[24]Using search engines data, Google and forensics - clip

Technorati tags :

[25]privacy,[26]search engine,[27]google,[28]MSN,  
[29]surveillance,[30]porn

Image originally uploaded at [31]Flickr by [32]villoks

1.

[https://web.archive.org/web/20101016193525im\\_/http://photos1.blogger.com/blogger/1933/1779/200/72599367\\_dc43a69e47.0.jpg](https://web.archive.org/web/20101016193525im_/http://photos1.blogger.com/blogger/1933/1779/200/72599367_dc43a69e47.0.jpg)

2. <http://blog.searchenginewatch.com/blog/060119-060352>

3.

<http://www.mercurynews.com/mld/mercurynews/13657303.htm>

4.

<http://blogs.msdn.com/msnsearch/archive/2006/01/20/515606.aspx>

5.

[http://www.theregister.co.uk/2001/05/31/what\\_are\\_those\\_words/](http://www.theregister.co.uk/2001/05/31/what_are_those_words/)

6.

<http://www.bugbrother.com/echelon/spookwordsgenerator.html>

7. <http://i.i.com.com/cnwk.1d/pdf/ne/2006/google-doj/motion.to.compel.pdf>

8. <https://adwords.google.com/select/main?cmd=KeywordSandbox>
9. <http://inventory.overture.com/d/searchinventory/suggestion/>
10. <http://www.alexa.com/>
11. <http://www.google.com/search?hl=en&lr=&sa=G&q=%22pichunter.com%22>
12. <http://www.marketresearch.com/>
13. <http://www.foxnews.com/story/0,2933,174828,00.html>
14. <http://www.mindbranch.com/products/R399-0158.html>
15. [https://web.archive.org/web/20101016193525/http://photos1.blogger.com/blogger/1933/1779/1600/google\\_P3P\\_privacy.0.jpg](https://web.archive.org/web/20101016193525/http://photos1.blogger.com/blogger/1933/1779/1600/google_P3P_privacy.0.jpg)
16. <http://ddanchev.blogspot.com/2006/01/still-worry-about-your-search-history.html>
17. <http://islandia.law.yale.edu/isp/regulatingsearch.html>
18. <http://www.p3ptoolbox.org/>
19. <https://web.archive.org/web/20101016193525/http://lorrie.cranor.org/>
20. <http://lorrie.cranor.org/pubs/pets04.pdf>
21. <https://web.archive.org/web/20101016193525/http://www.p>

[rivacybird.com/](http://privacybird.com/)

22. <http://lorrie.cranor.org/pubs/www06.html>

23. <http://blog.searchenginewatch.com/blog/060123-112156>

24. [http://media2.foxnews.com/111305/tech\\_google\\_111305\\_300.wmv](http://media2.foxnews.com/111305/tech_google_111305_300.wmv)

25. <http://technorati.com/tag/privacy>

26. <http://technorati.com/tag/search+engine>

27. <http://technorati.com/tag/google>

28. <http://technorati.com/tag/MSN>

29. <http://technorati.com/tag/surveillance>

30. <http://technorati.com/tag/porn>

31. <http://flickr.com/>

32. <http://flickr.com/photos/villoks/>

83

## **Security Interviews 2004/2005 - Part 1 (2006-01-26 07:22)**

I've decided to compile a list of all the interviews I have been taking for the [1]Asta's Security Newsletter (feel free to opt-in), with the idea to provide you with the opinions of **22** folks (two anonymous ones are excluded as perhaps they shouldn't have been taken at the first place, and a Xmas issue without an interview) that I have had the chance



to talk to. I hope you will enjoy the diversity of the their background and the topics covered.

Enjoy!

Go though [2]Part 2 and [3]Part 3 as well!

1. **Proge** - [4]<http://www.progenic.com/> - 2003
2. **Jason Scott** - [5]<http://www.textfiles.com/> - 2003
3. **Kevin Townsend** - [6]<http://www.itsecurity.com/> - 2003
4. **Richard Menta** - [7]<http://www.bankinfosecurity.com>[8] 2004
5. **MrYowler** - [9]<http://www.cyberarmy.net/> - 2004
6. **Prozac** - [10]<http://www.astalavista.com/> - 2004
7. **Candid Wuest** - [11]<http://www.trojan.ch/> - 2004
8. **Anthony Aykut** - [12]<http://www.frame4.com/> - 2004
9. **Dave Wreski** - [13]<http://www.linuxsecurity.com/> - 2004
10. **Mitchell Rowtow** - [14]<http://www.securitydocs.com/> - 2004
11. **Eric (SnakeByte)** - [15]<http://www.snake-basket.de/> - 2005
12. **Björn Andreasson** - [16]<http://www.warindustries.com/> - 2005
13. **Bruce** - [17]<http://www.dallascon.com/> - 2005
14. **Nikolay Nedyalkov** - [18]<http://www.iseca.org/> - 2005

15. **Roman Polesek** - [19]<http://www.hakin9.org/en/> - 2005
16. **John Young** - [20]<http://www.cryptome.org/> - 2005
17. **Eric Goldman** - [21]<http://www.ericgoldman.org/> - 2005
18. **Robert** - [22]<http://www.cgisecurity.com/> - 2005
19. **Johannes B. Ullrich** - [23]<http://isc.sans.org/> - 2005
20. **Daniel Brandt** - [24]<http://google-watch.org/> - 2005
21. **David Endler** - [25]<http://www.tippingpoint.com/> - 2005
22. **Vladimir, 3APA3A** - [26]<http://security.nnov.ru/> - 2005

-----

84

### **Interview with Proge, Founder of Progenic** [27]<http://www.progenic.com/>

**Astalavista** : To those who still don't know of Progenic.com, give us a brief introduction of the whole idea and its history?

**Proge** : Basically it all started in back in 98, we just made software for the fun of it and stuck it up on a webpage, mostly pretty simple stuff. It was a fun time but as the scene grew, things got a little out of hand, and when FakeSurf

(the first automated surfing tool) was released we had legal threats from Alladvantage, lost our sponsorship that was

paying for the bandwidth and were flooded with people wanting nothing more than a quick buck. I think that's when

everyone decided enough was enough, and we took the site behind closed doors, I left the toplist up on

Progenic.com because it's a scene I came from and I don't want to see it die. At the moment I'm

working on more constructive things like DownSeek.com, it's more satisfying to create something that helps people.

**Astalavista** : As being on the Scene for such a long time, what is your opinion on today's Security threats home and corporate users face every day?

**Proge** : There are usually two reasons why you become a target, automated software scanning your system for

known exploits that you should have patched, or you've made yourself a target. If someone wants to break into your

system then unless you have a dedication to security, that window between an exploit and a patch is going to get

you. Even if you stay on top

of things, it can still be a battle. According to Microsoft 'the only truly secure computer is the one buried in concrete, with the power turned off and the network cable cut' and you probably run their operating system.

**Astalavista** : Is Security through Education the perfect model for any organization?

**Proge** : Definitely! I'm still amazed that there are programmers and sys-admins out there, who think functionality first, security second or not at all. You need to understand hacking to understand Security, you know the reasons why you

lock your door at night, why you set an alarm, but do you know why you have a firewall or an intrusion detection

system, or did it just sound like a good idea when you got a glossy leaflet warning you about 'hackers' and asking

your money? You can't just install a product and forget about Security, but that's what the industry tries to

sell. Security is a constant threat and it isn't game over until you lose.

**Astalavista** : How real you think is the threat of CyberTerrorism?

**Proge** : With people like we have in power it gets more real. Like I said, if you make yourself a target, you've got a problem.

**Astalavista** : Is BigBrother really watching us, and what's the actual meaning of the word 'privacy' nowadays ?

**Proge** : A good question, they're definitely watching us but to what degree, who knows. It doesn't hurt to have a

healthy paranoia. There're two sides to the privacy argument really. Either you're worried that government/business

is overstepping the mark and intruding on your personal life for their own benefit, or you've got something to hide.

Unfortunately privacy is being marketed at those with something to hide, you've seen the ads, cheating on your

wife? Grooming underage kids? Erase your history, don't get caught etc. It's ironic that there are more ethics in a

scene that is largely banded a threat to Security than there are in government and business.

**Astalavista** : Thanks for your time, Proge.

**Proge** : You're welcome!

-----

85

**Interview with Jason Scott, Founder of TextFiles.com**  
**[28]<http://www.TextFiles.com/>**

**Astalavista** : How was the idea of TextFiles.com born?

**Jason** : TEXTFILES.COM was born because one day in 1998 I wondered what had ever happened to an old BBS I used

to call (it was called Sherwood Forest II). Since the WWW had been around for a good 5 years, I figured out there

would be a page up with information about it, and I could even download a few of the old textfiles I used to read

back in those days (the BBS was up from about 1983 to 1985). To my shock, there was nothing about Sherwood

Forest II anywhere, and nothing about ANY of the BBSes of my youth. So then I went off and registered the most

easy-to-remember name I could find, textfiles.com, and started putting up my old collection from Floppies. This gave

me about 3,000 files, which I used to attract other peoples' collections and find more on my own, until the curren

number, which is well past 60,000.

**Astalavista** : There's a huge amount of illegal and destructive information(bomb howto guides, drugs howtos)

spreading around the Internet these days.Some of these files can be found at TextFiles.com as well, don't you think

that accessing such information is rather dangerous and could endanger someone?

**Jason** : Well, the question makes it sound like this is a recent event, the availability of information that, if

implemented, could cause damage or other sorts of trouble. This has always been the case; if you want, we can go

back to the days of the TAP newsletter (and the later 2600 magazine) where all sorts of "dangerous" information was being printed. We can go back many years before that.

This may sound like a copout, but I don't really buy into the concept of "dangerous information". At a fundamental level, it is someone saying "I am looking at this, and I have decided you should not see it. So don't look. I've made my decision." And I find that loathesome in that it gives

someone enormous arbitrary power. This argument applies for the concepts of Obscenity and

Governmentally-Classified information, as well.

Sometimes people bring up the concept of children into the argument and my immediate reaction is not very

pleasant. Parents protect; be a parent.

If somebody wants to hurt somebody else, then information files are not the big limiting factor to them doing it;

they'll just pick up a match and set your house on fire, or buy a gun and shoot you or someone you really like.

Censorship, as you might imagine, is not big on my list of things

that improve the quality of life.

**Astalavista** : Nowadays Information could be considered the most expensive "good", what's your attitude towards the opinion that the access to certain Information would have to be a paid one?

Information is a very funny thing. It can be quantified to some extent, and some amount of control can be issued on

its transfer and storage. But the fact is that we, as a race, have been spending a lot of time making information

easier and easier to spread. Printing press, book, flyer, radio, records, tapes, CDs, DVDs, internet, Peer to Peer...

faster and faster. It is possible to know on the other side of the world what a child looked like at the moment it was

born, a mere few seconds later. When Americans elected the president in the 1800s, they might not know who had

won for weeks. Many people might have never seen a photograph of the man who ran

their country. They would almost certainly never hear him speak.

Charging for information is everyone's right. More power to them if they can make a buck. But that's not what I'm

talking about. I've seen kids with a hundred textfiles trying to sell access to them for \$5. If they're able to lure in

86

suckers to pay that, then they have a talent. When you're in the cinema, the same soda that cost something like fifty cents or a quarter, at the local store it will cost you two or three dollars. Are you paying for the soda or for the ability to have a soda in that location? Similarly, I don't think you're paying for the information on a site that charges,

you're paying a fee because you didn't know any other way to get this information.

There will always be a market for people with the ability to take a large amount of information and distill it for others (we called them "gatekeepers" when I took Mass Communications in college). The only difference is that now

anyone can be a gatekeeper, and people can choose to forget them and get the information themselves. So now it's an option, which is a great situation indeed.

I've always been insistent about not charging for access to textfiles.com and not putting advertisements up on the

site. I'm going to continue to do that as long as I can, which I expect will be for the rest of my life.

**Astalavista** : Share your thoughts about the Dmitry Skylarov case.

**Jason** : While this is not the first time that something like the Skylarov fiasco has occurred, I am glad that in this



particular instance, a lot of press and a lot of attention was landed on what was being done here. Adobe realized

within a short time that they'd made a serious mistake, and I hope they will continue to be reminded of how rotten

and self-serving they were in the whole event. I certainly hope the company name 'Adobe' will stay in the minds of

everyone with it for a long time to come.

That said, I'm glad everything worked out OK for him. Nobody deserves to be held up in a country away from their

family because some software publisher has decided they're evil.

America has occasionally taken poor shortcuts through very evil laws trying to fix problems and make them worse.

The "Separate but Equal" rulings in regard to Segregation and the indictment of anti-war protesters during World War I for something akin to Treason now have a modern cousin the DMCA and its equivalent laws, the Mini-DMCAs

being passed by states. I think we will look back at this time with embarrassment and whitewashing what went on.

**Astalavista** : How do you see the future of Internet, having in mind the Government's

invasion in the user's privacy, and on the other hand, the commercialization of the Net?

**Jason** : Mankind has been driven from probably day one to make things better, cheaper, and quicker because that's

what will bring them success and fortune. People talk about television being this vast wasteland of uselessness, yet

using something like my TiVO I can now bounce among my thousands of daily television programs and listen to

events and people that just 10 or 20 years ago, there would be no room on television for. For all the Internet's

abutments with the law, the fact is that it's still being adopted as fast as it can, the technology driving it is cheaper and cheaper (I have a connection to my house that costs me \$200 that would have cost upwards of \$10,000 in 1993)

and nobody is really able to say "This Internet Thing Needs to Go" and not get laughed at.

It took me years and years to collect the textfiles on textfiles.com. If people go to [torrent.textfiles.com](http://torrent.textfiles.com), they can

download the entire collection in as little as a few hours. People are now trading half-gigabyte to multi-gigabyte files like they used to trade multi-megabyte MP3 files just a few years ago.

I really don't have any fear about it being crushed. Too many people know the secret of how wonderful this all is. It's

a great time to be alive.

**Astalavista** : Thanks for the chat!

-----

**Interview with Kevin Townsend, Founder and Editor of [29]<http://ITSecurity.com>**

Originally taken for [30]HiComm Magazine

**Astalavista** : How did you get interested in the Information Security field?

**Kevin** : More by accident than design. I had been a freelance IT journalist for many years - then we had a child that couldn't sleep. We went through many, many months of averaging just a couple of hours sleep each night - it played

havoc with my freelancing; couldn't concentrate, couldn't write, couldn't meet deadlines... In the end I gave up and

got a proper job. It was actually the first thing that came along, and was marketing manager with a software

company that just happened to develop security software. But from then on I was hooked. Infosec is one of the

most fascinating areas there is: good versus bad, light versus dark - the perpetual battlefield at an intellectual level without any blood.

**Astalavista** : Share your viewpoint on the constantly increasing malware problem issue, are we going to see another ILOVEYOU disaster in the near future?

**Kevin** : I'm sure there will be more malware all the time - and sooner or later, one of them will be dramatic and

disastrous. My biggest fear for the Internet, however, is government intervention. Governments need control, and

they fear lack of control. The weaker they are, the more they need to control - and the world has some mighty weak

people in high office ATM. The Internet is a threat to their control. They need to control the Internet in order to

control people. Consider this: we call a category of malware 'viruses'. We do so because they behave like biological

viruses. If we continue that analogy, then the 'system' they attack (the Internet) equates to the human body.

Now, if a virus attacks a human, we react in several different ways. The 'traditional' method

(it isn't traditional at all; it's very recent) is to attack the virus with ever-stronger antibiotics, or even the surgeon's knife. But more and more of us are coming to the conclusion that this sort of 'quick fix' is no fix at all - all it does is weaken the immune system and encourage the virus to grow into ever stronger variants. The real solution is to

strengthen the immune system so that the viruses are tackled and destroyed without causing any damage.

This analogy should be passed back to computer viruses. If governments over-react with increasing penalties and

draconian actions (the surgeon's knife), we will weaken the Internet until it is just a pale shadow of the vibrant

organism it should be - and we still won't ever get rid of the viruses. The real solution is to strengthen the Internet, not to emasculate it.

**Astalavista** : As far as ITSecurity is concerned, what are the major

threats companies and home users face on a daily basis and how can they be prevented?

**Kevin** : Well, by now you won't be surprised to know that I consider over-regulation to be the major threat for both business and home users. We are all rapidly transferring our personas to the cyber world, whether that is our business persona or individual persona. Once that is complete, whoever controls the cyber world will control all of us. Smart card ID cards will be able to track everything that everybody does - in fact; we won't be able to do anything without the cards. And if a domain name is withdrawn, individuals or entire companies will effectively disappear overnight. This is a far greater threat than another Lovebug.

**Astalavista** : In today's world of terror, how real do you think the danger of

Cyberterrorism is, like stock exchanges going down, corporate networks completely devastated by terrorist groups?

**Kevin** : I think that the danger exists, but is over-hyped. Attack analyses show that a large percentage of attacks against western (that is, American) utilities and banks come from a very small number of countries well known to be

88

largely anti-American. I cannot believe that this is all done without their government knowledge - so the danger is very real. But just as there are some very clever people attacking systems, so there are some very, very clever people defending them.

**Astalavista** : What's your personal opinion on the US government's effort to monitor

its citizens' Internet activities, in order to protect them from potential terrorist attacks?

**Kevin** : It isn't, of course, just the US Government. I actually believe that the UK is already further down the line on this. Governments need to strike a balance between defending their people and enslaving their people. A recent

poll of American CSOs by CSO magazine shows

that 31 % of US business leaders believe that the USA is on the way to becoming a police state.

I think that most governments have failed to find the right balance - and I think the UK government has already put

everything in place for a police state in the UK. I forget the precise words, but the comment that 'those who would

give up freedom for security actually deserve

neither' is so very true.

-----

**Interview with Richard Menta**  
**[31]<http://BankInfoSecurity.com/>**

**Astalavista** : Hi Richard, I would appreciate if you introduce yourself and the web site you represent, namely

BankInfoSecurity.com

**Rich** : My name is Richard Menta. I work for an information security consulting firm in NJ called Icons, Inc where I serve

as a consultant and as the editor of BankInfoSecurity.com.

About 90 % of the Icons's clients are banks and credit unions. These institutions are heavily regulated regarding information security, yet despite this fact we found many of our clients needed much more education on the

concepts of information security and the added threats and risks presented by technology. BankInfoSecurity.com

was developed to help fill this need by aggregating the latest news and information, covering both the technical and regulatory aspects of InfoSec.

**Astalavista** : What's the major difference between the security threats the financial sector is dealing with, compared with the general security ones?

**Rich** : Privacy is the biggest issues with regards to financial institutions. They are mandated by the

Gramm-Leach-Bliley Act (GLBA) to protect what is called the non-public personal information (NPPI) of their

customers. The biggest security threat comes from intruders looking to garner NPPI to facilitate identity theft. As

the relationship of financial institutions with their customers is highly based on trust and mass identity theft

undermines that trust, it is a critical issue to control the theft of customer information.

**Astalavista** : E-business wouldn't be profitable without E-commerce, what do you think are the major security

problems E-shops face nowadays, how aware of the information security issue are the managers behind them, and

what do you think can make a significant change in their mode of thinking?

**Rich** : The biggest security issue is the lack of awareness as a whole. A good information security strategy takes significant effort and financial commitment, but many senior managers are unaware of the full breadth of what

information security covers. There is a lot to grasp too as information security is an every evolving discipline that has to rapidly change with the

changes in the threat environment.

89

Awareness is still an issue in the banking industry where there is a federal examiner coming in once a year to tell management what they need to do. The reason is because examiners have only been focused on information

security since 2001 (when the agencies started to enforce GLBA) and they are still learning the ins and outs. It's

improving, though, as examiners are visibly becoming savvier with time and communicating more to the banks.

Dramatic change in other industries is a bit more elusive as they have no such oversight as the banking industry does.

Still, the Sarbanes-Oxley Act looks to drive better information security because a deficient security plan violates the



due care requirements of the Act. As the act imposes criminal penalties for faulty compliance, there will be a lot more pressure once its tenets go into effect this fall.

**Astalavista** : Malicious software has always been trying to get hold of sensitive financial information, how significant do you think is the threat from worms like the Bizex one in future?

**Rich** : It is a significant problem as it goes back to the trust issue. All banks are adopting online banking, yet you have malicious code trying to take snapshots of your information as well as anyone else's who are in your address book.

The FDIC recently posted a mandate that banks must have a written patch management program consisting of

several steps. The reason the agency did this is because they realized that poorly patched systems posed a severe

threat and most financial institutions were doing an insufficient job with regards to patch activities. Right now, the

great majority of banks are

highly susceptible to these worms, as are their average customers who rarely patch their home systems. Of course,

even a great patch management program only goes so far, especially with zero day exploits.

**Astalavista** : Despite the latest technology improvements and the security measures put in place by companies, a

major part of the Internet users are still afraid to use their credit card online, who should be blamed and most

importantly, what do you think should be done to increase the number of online customers who want to purchase a good or services but feel secure while doing it?

**Rich** : Consumers are afraid for good reasons. How many prime trafficked sites have been broken? It is

embarrassing, especially when it makes the national media. The latest technology improvements and security

measures are good, but all merchants as a whole need to impose better security on their end. Those who don't

improve measures will continue to undermine the efforts of those who do by perpetuating the insecurity that many

patrons feel with regards to online shopping.

Again, it's a trust issue and there are a significant amount of consumers who don't trust typing their credit card

number into their browser. The good news is that as security improves throughout online commerce consumer trust

will rise.

**Astalavista** : What's your opinion on companies citing California's security breach disclosure law and notifying customers of a recent security breach?

**Rich** : Most companies can absorb any financial losses arising from a breach. It is the damage to their reputation

that poses the greatest risk. What is more embarrassing than notifying your customers their information was

compromised? Not only does the customer lose trust in the company, but such a disclosure inevitably becomes

public and that can hinder the ability to draw new customers.

So why do I think this law is good? Because there is a general apathy among many organizations regarding their

activities to properly protect their systems. Regulation has been the greatest motivator to improve security. In this

case, forced disclosure is far more motivating than any fine.

90

-----

### **Interview with Mr.Yowler, [32]<http://www.cyberarmy.net/>**

**Astalavista** : Mr.Yowler, Cyberarmy.com has been online since 1998, and is a well known community around the net.

But there're still people unaware about it, can you please tell us something more about the main idea behind

starting the site, and what inspired you the most?

**MrYowler** : Well, I didn't actually start the site; that was Pengo's doing. I actually joined when CyberArmy had about 37,000 members, and I worked my way up the ranks, first by completing the puzzles, and later by participating in the

community as one of its leading members. I was first put in charge, back in 2002, and I bought the domain from

Pengo, and completely took over, in late 2003.

CyberArmy is a community of 'hackers' of various skill levels and ethical colors. We focus primarily upon creating a

peer environment in which 'hackers' can share information and ideas, and we accomplish that through our Zebulun

puzzle and ranked forums, which serve to stratify discussion groups by comparative technical ability. We tend to

focus on 'n00bs', largely because they are the group that has the most difficulty finding peer groups to become

involved in, because they are the group that most often needs the technical and ethical guidance that CyberArmy

provides, and because they are the group that is most receptive to this guidance.

I suppose that what I find most inspiring about the CyberArmy is its tendency to regulate itself. People who are

interested in 'hacking hotmail' tend to gravitate together, and not pester people who are not interested in it, and

when they don't, the community rapidly takes corrective action on its own. This is a model that I would like to see

extend to the rest of the Internet; spammers and kiddie-porn dealers should be possible to identify and remove

from the networks without the necessity to monitor

\*everyone's\* email, through some regulatory or enforcement

organization that is largely unrepresentative of the users that it is chartered to protect.

I like that CyberArmy gives its members a reason to \*think\* about social ethics, and to decide upon what they

should be, rather than to simply accept what is established, without reasoning. I find that to be a fundamental

failing of modern society - that we frequently simply accept law, as the determinant of social ethics, instead of

requiring law to be guided by them. When people use \*judgement\*, rather than rely solely upon law, then people

are much more likely to treat one another with fairness. Externally imposed rules are for people who lack the

judgement skills to figure out how best to behave, without them. And most rules, today, are externally imposed. I

believe that when people \*think\* about social ethics, it usually results in a moral fiber that is founded in an honest

\*belief\* in the moral behavior that they come up with - and that this makes for infinitely better Internet citizens,

than rules or laws that are supported only by a deterrent fear of reprisals. I think that such people usually come up

with better behavior than the minimum standards that rules and law do, as well.

**Astalavista** : Cyberarmy runs a challenge - Zebulun, which happens to be a very popular one. How many people

have already passed the challenge, and what are you trying to achieve with it besides motivating their brain cells?

**MrYowler** : About 200,000 people have participated in the Zebulun challenge, over the years, to one extent or

another. Because the challenges are changed, over time (to discourage 'cheating', and to keep them challenging,

during changing times), the definition of "passed the challenge" is somewhat variable. Approximately 300-400

people have completed all of the challenges that were available to them, to obtain the highest possible rank that

one can reach, by solving the puzzles. That has traditionally been "Kernel" (the misspelling is an intentional pun) or

"General", and it is presently "Kernel". At the moment, the Kernel puzzle seems to be too advanced, and will probably have to be changed. There are seven puzzles, and our intended target is that there should always be about

a 2:1 ratio of players, from one rank to the next. This guarantees that the puzzles will be challenging to most players, 91

without being discouraging.

Of course, we like encouraging people to learn. More importantly, I'm trying to get people to \*think\*. Anyone can

become educated about technical systems; this only requires time and dedication to the task. And while that is an

important thing to do, it is already heavily stressed in schools, and throughout most societies and cultures. Smart

people know a lot of things.

But this is not entirely true. Most smart people have come to realize that "knowledge is power" - but it is not the knowledge that makes them smart. As with static electricity, which is expressed only as voltage potential - until it

strikes the ground as lightning - knowledge is not expressed as power, until someone \*thinks\*, and applies that

knowledge to some useful purpose. Socrates was effectively an illiterate shoe-salesman (a cobbler), but he is

considered a great philosopher, because he took the little bit that he knew about the world, and \*thought\* about it.

Not only that, but he convinced others to think about it, as well. Einstein was a mediocre mathematician and

generally viewed as a quack, until his thinking was expressed in the form of nuclear energy. \*Thought\* is what

separates the well-educated from the brilliant - and most successful 'hackers' rely much more upon \*thought\*, than

upon an exhaustive understanding of the systems that they target. Not that having such knowledge isn't helpful... :)

I am trying to get people to \*think\* - not only about intrusion tactics, but also about defensive measures,

motivations, risks, ethics, and about life in general. Too much of the world around us is taken for granted, and not

questioned. Not thought about. I am trying to make the art of questioning and \*thinking\*, into a larger part of

people's lifestyles.

**Astalavista** : How did the infosec industry evolved based on your observations since 1998? Is it getting worse? What are the main reasons behind it? Crappy software or the end users' lack of awareness?

**MrYowler** : In its early years, the infosec industry was largely dominated by the mavericks - as is true with most developing industries. A few people dominated the profession, with their independence - it gave them the freedom

to tell the business world how things should be, and to walk away, if the business world was unwilling to comply.

Today, we see less of that, and

while the industry is still largely dominated by such people, the majority of people whose job is to implement system

security, are much more constrained by resource limitations.

Essentially, there are two groups of people in the defensive side of this industry; the policy-makers and the

implementors. Policy-makers are usually corporate executives, CISOs, legislators, consultants, or otherwise figures

of comparative authority, whose job it is to find out what is wrong with system security, and to come up with ideas

about how to fix it. Implementors are usually the ones who are tasked with implementing these ideas, and they are

usually system or network administrators, programmers, security guards, or otherwise people whose influence on



things such as budget and staff allocation, is insignificant. As a rule, the policy-makers make a great deal of money, establishing policies that they have very little part in implementing, and often these policies have a significant impact upon the work loads and environments of implementors.

It is all well and good, for example, to decide that there will be no more use of instant messenger software in the workplace. Stopping it from occurring, however... while remotely possible, by employing purely technical measures, it is certainly not desirable or inexpensive. Even monitoring for it can require staff resources which are rarely allocated for the task, and the effect of draconian security measures - or penalties for non-compliance - is usually much more damaging to workplace productivity than the instant messengers ever were. For some reason, policy-makers have abandoned the basic principle of system design; "involve the user" - and have limited themselves to requiring the support of executive management. Security policy is surprisingly cheaper, faster, and easier to achieve compliance with, when it also has the support of the rank-and-file members of an organization - and not the kind of support that is achieved putting a professional gun to their heads, by requiring

people to sign compliance agreements. Rather, the support that is achieved by giving the employees a sense of personal investment in the security of the system. User awareness is fairly easy to achieve, although users will tend

to disclaim it, when caught in a violation or compromise. Creating accountability documents, such as security policy

compliance agreements, may combat these disclaimers; but the most truly effective approach is not to just tell the

users and demand compliance - but to give the users a voice in it, and the desire to strive for it. In many cases, the

users have excellent ideas about areas where system security falls down - and similarly excellent ideas about how to

fix it.

Policy-makers have to bridge the gap between themselves and implementors, or security will always be 'that

pain-in-the-ass policy' which people are trying to find ways to work around. And instead of the draconian Hand of

God, which appears only so that it can smite you down; security needs to become the supportive friend that you can

always pick up the phone and talk

to, when you have a question or a problem.

That having been said, there is another problem with modern security practices, that is worth giving some attention

to...

Because security has traditionally been sold to organizations, as a way to prevent losses that result from security

compromises, these organizations have begun to assign values to these compromises, and these values determine

the extent to which these organizations will go, to prevent them. While perfectly reasonable and sensible from a

business perspective, these values are determined largely by educated guessing, and the value of a compromise can

be highly subjective, depending upon who is making the assessment.

Remember - if your credit information gets into the hands of someone who uses it to print checks with your name

on them, you could spend years trying to straighten out your credit with the merchants who accept these checks. It

can impact your mortgage interest rates, or prevent you from getting a mortgage, at all - and it can force you to carry

cash, in amounts that may

place you in considerable personal danger. The organization which pulls a credit report on you, to obtain this

information, however, stands very little to lose from its compromise, since you are unlikely to ever determine, much

less be able to prove, that they were the source of the

compromise. So, what motivates them to guarantee that all credit report information is properly protected,

destroyed and disposed of? What's to stop them from simply throwing it in the garbage? And what happens to it, if

they go out of business, or are bought out by some other company? To what extent do they verify that their

employees are trustworthy?

This\* is typically where security falls down. Remember; security is the art of protecting \*yourself\* from harm - not

necessarily your customers, your marketing prospects, or anyone else. As a result, most of the effort to secure

systems, goes into protecting the interests of the people who \*operate\* those systems - and not necessarily the

users of them, or the data

points that they contain information about. In many cases, legal disclaimers and transfers of liability replace actual

protective countermeasures, when it comes to protecting things that \*you\* care about - and in still other cases, a

lack of accountability suffices to make an

organization willing to take a chance with your security, out of a commercial interest in doing so. Marketing entities

often openly sell your information, or sell the use of your information to market things to you, and make no bones

about doing so - after all, it's not their loss, if your

information gets misused - it's yours.

This is a fundamental problem in information security, and for many of us it costs our personal freedom. The

government needs access to all of our emails, without the requirement to notify us or get a warrant to access the

information, because we might be drug dealers or child molesters. And I worry that some child molestor will gain

93

access to the information, through

the channels that are made available to government.

Amazon.com stores our credit information, in order to make is

easier for us to buy books through them, in the future - and I worry that all someone needs is the password to my

Amazon.com account, to start ordering books on my credit card. Every time that I fill out an application for

employment, I am giving some filing

clerk access to all the information required, to assume my identity. That information is worth a great deal, to me -

how much is it worth, to them? Enough to pay for a locking cabinet, to put it into? Enough to put it into a locked

office? Enough to alarm the door? Enough the get a guard to protect the facility in which it is stored? Enough to arm

the guard? Enough to adequately shred and destroy the information, when they dispose of it? Enough to conduct

criminal background investigations on anyone that has access to the information? Or do they just get some general

corporate liability insurance, and figure that it's an unlikely-enough circumstance,

that even if it happens, and I'm able to trace it back to them, and make it stick, in court, that it's worth the risk of a nuisance liability lawsuit?

At its core, information security is failing, for at least these two reasons: 1) for all the talk that goes on, very little on the way of actual resources are devoted to information security; and, 2) people and organizations usually show

comparatively little interest in anyone's security but their own.

**Astalavista** : Mr.Yowler, lately we've seen an enormous flood of worms in the wild,

what do you think is the reason?

**MrYowler** : Firstly, these worms exploit errors in upper-layer protocols of networks and

network applications. Because network applications are proliferating at an ever-increasing rate, the possible ways to

exploit them are also increasing at this geometric rate - and people who are interested in exploiting them, therefore

have more things to work with.

Secondly, there is a glut of information technology talent in the United States, perhaps thanks, in part to the collapse of

the Internet economy - and also, in part, thanks to the rush to outsource technology jobs to overseas entities.

Additionally, third-world countries have been developing technical talent for some years, now, in an effort to become competitive in this rapidly-growing outsourcing market.

This has created an environment where technical talent is plentiful and cheap - and often disenfranchised.

In some cases, these worms are written by kids, with nothing better to do - and that has always been a problem,

which has grown in a linear way, as more and more advanced technical education has begun to become available to

younger and younger students.

In other cases, this is the technical equivalent of "going postal", in which a disenfranchised technology worker creates a malicious product, either as a form of vengeance, or in the hope of creating a need for his own technical

talents, as a researcher of considerable talent, with regard to the worm in question. Surprisingly many people who

might otherwise never find work in

the technical or security industries, are able to do so, by making a name for themselves through criminal activity or

other malicious behavior. While demonstrating questionable ethics, it also demonstrates technical talent, and the

notoriety is sometimes more valuable to a company, than the damage that they risk by hiring someone whose ethics

are questionable. Many people

are employed or sponsored in the lecture circuit, for this reason; they did something that bought them notoriety -

good or bad - and their employer/s figure that they can benefit from the notoriety, without risking a lot of possible

damage, by putting these people on the lecture circuit.

In an increasing number of cases, these disenfranchised technology workers are actually employed for the specific

purpose of creating malware, by spyware, adware, and spam organizations, as I will cover in the next question.

94

When one is forced to choose between one's ethics and feeding one's children, ethics are generally viewed as a luxury that one can no

longer afford. I, myself, am currently under contract to a spammer, since I am now approximately two weeks from

homelessness, and better offers have not been forthcoming. I'm writing an application which will disguise a process

which sends out spam, as something benign, in the process listing, on what are presumably compromised \*nix hosts.

The work will buy me approximately one more week of living indoors, which is really not enough to justify the

evil of it, but I am in no position to refuse work, regardless of the employer. And indeed, if I did not accept the



contract, and cheaply, then it is quite likely that someone from a third-world country would have done so - and

probably much more cheaply than I did.

**Astalavista** : Recently, spammers and spyware creators started using 0-day browser

bugs, in order to disseminate themselves in ways we didn't consider serious several months ago. Did they get

smarter and finally realize the advantages of a 0-day exploit, compared to those of an outdated and poisoned e-mail

database?

**MrYowler** : As indicated in the previous question, spam, spyware and adware organizations are beginning to

leverage the fact that there is now a glut of technical talent available on the world market, and some of it can be

had, very cheaply. These organizations have been taking advantage of technical staff that could not find better work

for a long time. As more people who

possess these talents, find themselves unable to sustain a living in the professional world; they are increasingly likely to turn to the growing professional underground.

Employment in the security industry is no longer premised on talent, ability, education, skill, or professional

credentials, and there are essentially three markets that are increasingly reachable, for the malware professional

world. 1) Third-world nations with strong technical educational programs are simply screaming for more of this sort

of comparatively lucrative work to do. 2) Young people who lack the age or credentials to get picked up

professionally, by the more respectable organizations, often crave the opportunity to put 'hacking' skills, developed

in earlier years, to professional use. 3) Older technology workers, finding it difficult to find work in a market

dominated by under-30-year-old people, often have large mortgages to pay, and children to put through college, and

are willing to take whatever work they can find - if not to solve their financial problems, then perhaps to tide them

over until a better solution presents itself.

It's not so much that spam, spyware, and adware marketers have become smarter, as it is that greater technical

talent has become available to them. The same people who used to develop and use blacklists, and filter spam

based upon header information for ISPs that have since gone bankrupt or been bought out, are now writing worms

that mine email client databases, to

extract names and addresses, and then use this, combined with email client configuration information, to send

spam out from the user's host that the addresses were mined from. They are using the user's own name and email

address, to spoof the sender - even using the SMTP server provided to the victim, by their ISP, to deliver the mail.

This effectively permits them to

relay through servers that are not open relays, and distributing the traffic widely enough to stay under the

spam-filtering radar of the sending ISPs, and to evade the blacklisting employed by the receiving ISPs. It also permits

them to leverage the victim's relationship to the recipients of the spam, in order to get them to open and read it -

and sometimes, to get them to open attachments, or otherwise infect themselves with the worm that was used to

reach them. The spammers have not previously been able to hire talent of this grade, very often - now, this talent is

often not only available, but often desperate for cash, and therefore willing to work cheap.

It's a bit like an arms race. In the rush to develop enough technical talent to defend against this sort of thing, we

have developed an over-abundance of talent in the area - and that talent is now being hired to work against us. This

will presumably force people to work even harder at developing countermeasures, and repeat the cycle.

Assuming,

95

of course, that the threat is taken seriously enough by the public, to keep the arms race going. After all - once

everybody has enough nuclear weapons to destroy all the life on Earth, then there isn't much point in striving to

build more. You just have to learn to deal with the constant threat of extinction, and try

not to take it too seriously - since there isn't really anything to be done about it, any more. We seem to be rapidly

approaching this mentality, with regard to malware.

**Astalavista** : What is your opinion on ISPs that upgrade their customers' Internet connections for free, while not providing them with enhanced security measures in place? To put it in another way, what do you think is going to

happen when there're more and more novice ADSL users around the globe, who don't have a clue about what is

actually going on?

**MrYowler** : This comes back around to the second point, with regard to the problems of

information security, today. People have little interest in anyone's security but their own.

The ISPs \*could\* block all outgoing traffic on port 25, unless it is destined for the ISPs SMTP servers - and then

rate-limit delivery of email from each user, based upon login (or in the case of unauthenticated broadband, by IP

address). This is a measure that would have effectively

prevented both the desktop server and open relay tactics that I described in my paper, "Bulk Email Transmission

Tactics", about four years ago, and it would severely constrain the flow of spam from zombie hosts in these user

networks. The problem is that they don't care. They only care when the spam is \*incoming\*, and then they can

point fingers about how uncaring someone else is. The same holds true for individual users.

It is neither difficult nor expensive to implement a simple broadband router, to block most incoming traffic which

would be likely to infect user hardware with malware. It is also not difficult or expensive to implement

auto-updating virus protection, spyware/adware detection/removal, and software patching. It could be done even

more cheaply, if ISPs were to

aggregate the costs, for all of their users, and buy service contracts for this kind of protection, in bulk, for their users, and pass the cost along as part of the 'upgraded' service. Unfortunately, the nominal cost of doing so, would have to

be borne by users who do not take the threat seriously, and who only care about the threat, when it has a

noticeable impact on them. Since many of the malware packages are designed \*not\* to have a noticeable impact on

the user - using them essentially as a reflection, relay, or low-rate DDoS platform, or quietly extracting data from

their systems which will be abused in ways not directly traceable to their computer - these users do not perceive the

threat to be real, and are therefore unwilling to invest - even nominally - in protecting themselves from it. ISPs are

not willing to absorb these costs, and they are not willing to risk becoming uncompetitive, by passing costs on to

their subscribers; so they pay lip service to questions of security and antispam service, and perform only the most

minimal tasks, to support their marketing claims.

As with most organizations, the security of the organization itself, lies at the focus of their security policies. The

security of subscribers, other network providers, or other Internet users in general, is something that they go to

some trouble to create the perception that they care about, but when the time comes to put their money where

their mouths are, it's just not happening.

**Astalavista** : Thanks for your time.

**MrYowler** : Any time... :-P

-----

**Interview with a core founder of Astalavista.com**  
**[33]**<http://www.astalavista.com/>

**Dancho** : Hi Prozac, Astalavista.com - the underground has been one of the most popular and well known

96

hacking/security/cracks related web site in the world since 1997. How did it all start? What was the idea behind it?

**Prozac** : Basically, it was me and a college friend that started Astalavista.com during our student years. The name of the site came from the movie Terminator 2 from Schwarzenegger's line " Hasta la vista Baby"! Back in those days there weren't many qualified security related web sites, and we spotted a good opportunity to develop something

unique, which quickly turned into one of the most popular hacking/security sites around the globe. In the beginning,

it was just our Underground Search List, the most comprehensive and up-to-date search list of underground and

security related web sites, based on what we define as a quality site. Then we started providing direct search

opportunities and started developing the rest of the site. Many people think we did some serious brainstorming

before starting Astalavista, well, we did, but we hadn't expected it to become such a popular and well known site,

which is the perfect moment to say thanks to all of you who made us as popular as we're today.

**Dancho** : Astalavista.com always provides up to date, sometimes "underground" documents/programs. The Security Directory is growing daily as well, and it has been like this for the past several years. How do you manage to keep

such an archive always online, and up to date?

**Prozac** : Astalavista's team members are aware of what's "hot" and what's interesting for our visitors, just because we

pay an enormous attention to their requests for security knowledge, and try to maintain a certain standard, only

quality files. While we add files every day, a large number of those are submitted by our visitors themselves, who

find their programs and papers highly valued at our site, as we give them the opportunity to see how many people

have downloaded their stuff.

**Dancho** : Astalavista occupies people's minds as the underground search engine. But what is Astalavista.com all about?

**Prozac** : The majority of people still think Astalavista.com is a Crack web site, which is NOT true at all.

Astalavista.com is about spreading security knowledge, about providing professionals with what they're looking for,

about educating the average Internet user on various security issues; basically we try to create a very well

segmented portal where everyone will be able to find his/her place. We realize the fact that we're visited by novice,

advanced and highly advanced users, even government bodies; that's why we try to satisfy everyone with the files

and resources we have and help everyone find precious information at astalavista.com. Although we sometimes list

public files, the exposure they get through our site is always impressing for the author, while on the other hand,



some of the files that are listed at Astalavista.com sometimes appear for the first time at our site. We try not to emphasize on the number of files, but on their quality and uniqueness.

**Dancho** : Everyone knows Astalavista, and sooner or later everyone visits the site. How did the image of Asta become so well-known around the world?

**Prozac** : Indeed, we are getting more and more visitors every month, even from countries we didn't expect. What

we think is important is the quality of the site, the lack of porn, the pure knowledge provided in the most

professional and useful way, the free nature of the site, created "for the people", instead of getting it as commercial as possible. Yes, we work with a large number of advertisers, however, we believe to have come to a model where

everyone's happy, advertisers for getting what they're paying for, and users for not being attacked by adware or

spyware or a large number of banners.

**Dancho** : A question everyone's asking all the time - is Astalavista.com illegal?

**Prozac** : No! And this is an endless debate which can be compared to the Full Disclosure one. We live in the 21st

century, a single file can be made public in a matter of seconds, then it's up to the whole world to decide what to do

with the information inside. We're often blamed because we're too popular and the files get too much exposure.

We're often blamed for serving these files to script-kiddies etc. Following these thoughts, I think we might also ask, is Google illegal, or is Google's cache illegal?! Yes, we might publish certain files, but we'll never publish "The Complete Novice Users on HOWTO ShutDown the Internet using 20 lines VB code". And no, we don't host any

cracks or warez files, and will never do.

**Dancho** : Such a popular security site should establish a level of social responsibility - given the fact how popular it is among the world, are you aware of this fact, or basically it's just your mission that guides you?

**Prozac** : We're aware of this fact, and we keep it in mind when approving or adding new content to the site. We also realize that we still get a large number of "first time visitors", some of them highly unaware of what the security world is all about; and we try to educate them as well. And no, we're not tempted by "advertising agencies" eager to place adware/spyware at the site, or

users submitting backdoored files, and we have a strict policy on how to deal with those - "you're not welcome at

the site"!

**Dancho** : We saw a completely new and "too professional to be true" Astalavista.com since the beginning of 2004 -

what made you renovate the whole site, and its mission to a certain extend?

**Prozac** : It was time to change our mission in order to keep ourselves alive, and most importantly, increase the

number and quality of our visitors, and we did so by finding several more people joining the Astalavista.com team,

closely working together to improve and popularize the site. We no longer want to be defined as script kiddies

paradise, but as a respected security portal with its own viewpoint in the security world.

**Dancho** : What should we expect from Astalavista.com in the near future?

**Prozac** : To put it in two words - changes and improvements. We seek quality and innovation, and have in mind that these developed by us, have an impact on a large number of people - you, our visitors. Namely because of you we're

devoted to continue to develop the site, and increase the number of services offered for free, while on the other

hand provide those having some

sort of purchasing power and trusting us with more quality services and products.

**Dancho** : Thanks for the chat!

**Prozac** : You're more than welcome :)

-----

**Interview with Candid Wuest,**  
**[34]<http://www.trojan.ch/>**

**Astalavista** : Candid, would you, please, introduce yourself to our readers and tell us more about your background in the security industry?

**Candid** : Well, my name is Candid and I have been working in the computer security field for several years now, performing different duties for different companies. For example, IBM Security Research and Symantec to name the most known ones. I got a master degree in computer science but, in my opinion, in this business curiosity is the main thing that matters.

**Astalavista** : What do you think has had a major impact on the popularity of malware in recent years? Is it the easiness of coding a worm/trojan or the fact that the authors don't get caught?

98

**Candid** : Why do people code worms? Because they can?

The first point I would like to mention here is the growth of the Internet as a whole in the last years. More people

getting a system and more people getting broadband access means more people are exposed to the risks. You may

say the fish tank has grown over the years; therefore it is clear that there is now also more space for sharks in it.

I think the few people which where caught have scared some and stopped them from doing the same, but the

media hype they have caused has for sure attracted new ones to get started with the whole idea. So this might

balance out even and these were mostly smaller fishes, which didn't take enough precautions.

Another point to mention is that it is really easy to download a source code and create your own malware and it is

getting easier every day. There are many bulletin boards out there with fast growing communities helping each

other in developing new methods for malware or simply sharing their newest creations.

When recalling the last hundreds of worms we saw in the wild for the last time, most of them were similar and much

alike. Nearly no direct destructive payload and not much innovation in regards to the used methods. Just a mass

mailer here or an IRC bot there.

That's why I think the motivation is a mixture of the easiness of doing so and the mental kick suggested from the

media, which pushes the bad underground hacker image. (Even though the media uses the term hacker seldom

correctly in its original meaning.) This seems to motivate many to code malware: just because they can.

In the future money might become a new motivation for malware writers, when industrial parties get involved in it.

**Astalavista** : Where's the gap between worms in the wild and the large number of infected computers? Who has

more responsibility, the system administrators capable of stopping the threat at the server level, or the large number

of people who don't know how to protect themselves properly?

**Candid** : As we all should know 100 % security will never be reached, regardless of what the sysadmin and the end

user do. A good example for this is the recent issue with the JPEG and TIFF malware, which sneaked through many filters.

In my opinion the sysadmins have the easier task, as they can enforce their restriction; often it's just a question of

having the time to do it properly. Don't get me wrong here. I know the whole patching issue may be quite a pain

sometimes. Of course, they have all the users and the

management complaining if the restrictions are (too) tight but that's how it works, right :- )

Therefore I think often it is the end user who has not enough protection or simply does not care enough about it.

Many users still think that no one will aim at them, as they are not an interesting target, but DDoS attacks for

example do exactly target such a user. Of course, many end users don't have the possibilities of a sysadmin. In

general, it comes down to an AntiVirus and a personal firewall application, which still leaves enough space for

intruders to slip through.

So, as always, it should be a combination of an ISP, a sysadmin and an end user working together to protect

themselves.

**Astalavista** : We've recently seen a DDoS mafia, something that is happening even now. What is the most

appropriate solution to fight these? Do you think this concept is going to evolve in time?

**Candid** : DDoS attacks are quite hard to counter if they are performed in a clever way. I have seen concepts for

99

which I haven't seen a working solution yet. Some can be countered by load balancing and traffic shaping or by simply changing the IP address if it was hard coded. More promising would be if you could prevent the DDoS nets

from being created, but this goes back to question number three.

**Astalavista** : Have you seen malware used for e-spionage, and do you think it's the next trend in the field?

**Candid** : This is nothing new; malware has been used for industrial e-spionage for years. Usually, it just isn't that well known as those attacks might never get noticed or admitted in public. I have seen plenty of such attacks over

the last years. This for sure will increase in time as more business relevant data gets stored in vulnerable

environments. In some sort you could even call phishing an art of espionage. But I think the next big increase will be

in the adware & spyware filed where malware authors will start getting hired to write those applications as

it already happens today. Or are you sure that your favourite application is not sending an encoded DNS request

back somewhere?

-----

### **Interview with Anthony Aykut, Frame4 Security Systems [35]<http://www.frame4.com/>**

**Astalavista** : Anthony, would you please tell us something more about your experience in the InfoSec industry, and what is Frame4 Security Systems all about?

**Anthony** : Sure. I guess I am what you would primarily call a "security enthusiast", with what I came to see as "a keen sense of security business enthusiasm". Actively following the Trojan/Virus community since my teens in the

late-1980's, I have been working in the IT industry since the early 90's, though up until 2002 I have never felt the

need to follow the IT security path. Let's just say that a certain chain of events made me "fall" into it :-)) ... and that is when I decided to start Frame4 Security Systems.

Frame4 Security Systems is a small IT-Security company based in the Netherlands. We offer the usual

"out-of-the-box" professional security services (security audits, pen-testing, etc.), but we especially pride ourselves on our outstanding security awareness programs (seminars and

courses), exceptional service, and our upcoming "ProjectX Security Knowledgebase". I really feel that we are on an



unique playing-field with Frame4; whereas big (and often expensive) consultancies are primarily focused on big

companies/contracts, bottom line figures and dead-lines - often the Security Awareness on a personal (employee)

level gets often overlooked. This creates a well-known security gap that gets exploited more and more often,

rendering the million-dollar security solution back in the server-room absolutely useless. I have personally seen

good examples of this within big companies - and it is therefore we let the big boys do what they are good at by

providing solid, proven solutions, whereas we have the unique opportunity of "fighting the disease from inside-out".

**Astalavista** : "Internet privacy", do these words still exist in your opinion?

**Anthony** : To a large extent (and unfortunately), no. But I guess this was to be expected with millions of people

pumping their personal data into online databases and keeping information on their PCs. It is an open field, with

little or no control or control structure. Let's face it, (personal) information and data is big business, and people will do absolutely anything from hacking databases to infecting people with spyware/trojans to extract that information.

And in some cases, custodians of personal information have just made it way too easy for other (unauthorised)

people to gain access to private data. I guess that's when the finger-pointing started :-)

But on a more serious note, I have friends who are so paranoid that they only surf the net behind a wall of proxies and anonymizers, under false/assumed names and identities. Me, I am just careful; I think when people have a basic

online awareness level, and know what to look out for, it is no more a threat to your information than, say, putting

your garbage outside and someone going through it (a.k.a. dumpster diving).

100

**Astalavista** : We have recently seen a large number of DDoS extortion schemes, whereas certain companies comply behind the curtains, should we consider every E-business site that goes down a victim of extortion schemes? What

do you think a company should do in a situation like this?

**Anthony** : I personally think that "head-in-the-sand" ostrich attitude is completely wrong; pay once to one extortionist, and a dozen others will line up to grab that easy cash. I don't think you should comply and give in to any of these demands (I prefer to call them threats) but come out with it in the open and track down the perpetrators if

possible. Openness, like some companies have chosen, may possibly dent your corporate identity on a temporary

basis, but also takes away the power of the extortionist. We have seen that this approach is the lesser of two evils in

general, especially true if your business does not depend on a internet presence per se.

**Astalavista** : In today's world of "yet another worm in the wild", what do you think are the main consequences for this cycle, and what do you think should be done in order to prevent it?

**Anthony** : Well, I am pretty clear on that. As long as publicly/privately available source-code floats around the web, not much can be done - unless the AV vendors come up with better technologies. It really is up to them to come up

with better and improved techniques to protect our systems - more and more the current AV technology is showing

that it is getting out-dated by being circumvented in many ways. I am more than aware that it is difficult to "protect against the unknown", but I just know there should be more. Maybe AV vendors should float a bit more within the

"community" to gain awareness

:-)

To be honest, with the advent of other malware, such as Trojans, Sniffers, Keyloggers and Spyware to name a few

and many interesting technologies such as Firewall-Bypassing, etc. it is getting more and more obvious that we need

an "All Comprehensive Malware Solution" than just a pattern based AV system. It just ain't cutting it anymore. Until then, keep up your defences and update those virus patterns on a daily basis!

**Astalavista** : The threat and actual infections with spyware opened up an entire market for anti-spyware related

services and products, whereas millions of people out there are still infected, and some are even unaware of it.

What is your opinion on the recent government regulations targeting spyware vendors, but allowing "spy agencies"

to use spyware? What do you think is going to happen on the spyware scene in the next couple of years?

**Anthony** : Well, as I pointed out in your previous question, I tend to see Spyware almost in the same category as

Trojans, Viruses and other malware. Subsequently I think things are going to get (much) worse before they (I hope,

eventually) get better, and it is going to take some considerable changes in AV technology for one (along with our

ways of thinking) to ensure people will not take advantage of these technologies to the disadvantage of others.

Currently things are not looking too good: governments have proven that we cannot trust their ineffective and

inevitably slow schemes and until better/additional technologies are invented to bolster our AV defences, we are

pretty much sitting duck targets. This has been proven yet again with the recent "hijacking" of 1000's of

zombie/drone PCs to perform DDoS attacks, etc. So it is really up to the individuals to get at least some basic

security measures up and running, and there are plenty of reputable web-sites out there to provide all the

information one needs to secure themselves well.

**Astalavista** : Thanks for your time.

**Anthony** : No problem!

-----

101

**Interview with Dave Wreski,**  
**[36]<http://www.linuxsecurity.com/>**

**Astalavista** : Dave, tell us something more about your background in the InfoSec industry and what is

LinuxSecurity.com all about?

**Dave** : I have been a long-time Linux enthusiast, using it before version v1.0 on my 386DX40 home PC, which

prompted me to dump Windows shortly thereafter and I've never looked back.

In early 1993 I began to realize the tremendous value that Linux could bring to the security issues I was facing. I

found the decisions I was making, with regard to managing computer systems, were more and more based on the

impact security had on the data residing on those systems. It's certainly more challenging to keep the bad guys out

than it is the other way round - the bad guys have to only be right once, while the good guys have to always make

the right decisions. So I created a company to help ensure the good guys had the tools necessary to make the most effective options to keep their networks secure.

The void in comprehensive information on security in the Linux space was the primary reason I started

LinuxSecurity.com in 1996. Since then, we have seen millions of visitors make it their primary information resource.

In fact, we're completely revamping the site with new features, greater functionality and a whole new look

-launching December 1st.

**Astalavista** : What was the most important trend in the open-source security scene during the last couple of years,in your opinion?

**Dave** : Actually, there have been so many that it's difficult to focus on any one in particular. Certainly, the adoption of open standards by many vendors and organizations makes it much easier to communicate between disparate

systems securely. The maturity of the OpenSSH/OpenSSL projects, IPsec, and even packet filtering has enabled

companies, including Guardian Digital, to create solutions to Internet security issues equal to, or better than, their proprietary counterparts.

**Astalavista** : The monopolism of Microsoft in terms of owning more than 95 % of the desktops in the world has

resulted in a lot of debates on how insecure the whole Internet is because of their insecure software. Whereas my

personal opinion is that if Red Hat had had 95 % of the desktop market, the effect would be the same. Do you think their

software is indeed insecure, or it happens to be the one most targeted by hackers?

**Dave** : I think the mass-market Linux vendors try to develop a product that's going to provide the largest numbers of features, while sacrificing security in the process. They have to appeal to the lowest common denominator, and if

that means delivering a particular service that is requested by their customers, then much of the responsibility of

security falls on the consumer, who may or may not be aware of the implications of not maintaining a secure system,

and in all likelihood, do not possess the ability to manage the security of their system.

**Astalavista** : The appearance of Gmail and Google Desktop had a great impact on the privacy concerns of everyone,

however these expenditures by Google happened to be very successful. Do you think there's really a privacy

concern about Google, their services and privacy policy, and, most importantly, the future of the company?

**Dave** : No, not really. I actually think that most of us gave up our privacy years ago, and any privacy that remains is only in perception. There's far more damage that could be done

through things like the United States Patriot Act than there is through Google reading your general communications.

Anyone who has half a brain and wants to make sure their communications are not intercepted is using cryptography for electronic issues.

102

**Astalavista** : We've recently seen an enormous increase of phishing attacks, some of which are very successful.

What caused this in your opinion? What is the way to limit these from your point of view?

**Dave** : Reduce the human factor involvement somehow. Phishing is just the new "cyber" term for social engineering, which has existed forever. Through the efforts of Guardian Digital, and other companies concerned about the

privacy and security of their customers' data, we are making great strides towards user education, and providing

tools for administrators to filter communications.

**Astalavista** : Spyware is another major problem that created an industry of companies fighting it, and while the

government is slowly progressing on the issue, the majority of PCs online are infected by spyware. Would you,

please, share your comments on the topic?

**Dave** : This issue is different from issues such as phishing because the end-user is not aware it is occurring. The responsibility here falls directly on the operating system vendor to produce an



environment where security is maintained. In other words, by creating software that enables the end-user to better

define what constitutes authorized access, users can develop a situation where this type of attack does not succeed.

In the meantime, application-level security filters and strict corporate information policies thwart many of these

types of attacks.

**Astalavista** : What do you think will happen in the near future with Linux vs. Microsoft? Shall we witness more Linux desktops, or entire countries will be renovating their infrastructure with

Unix-based operating systems?

**Dave** : We are already seeing a growing trend on an international level in the migration from Windows operating systems to Linux. Guardian Digital has implemented several Linux-based solutions for multi-national and

international corporations who recognize the costs and security risks associated with a Windows system, and if our

business is any indication of the growth potential, I'd say Microsoft is going to have a real fight on their hands.

Although I'm not too involved in the desktop space itself, I am completely comfortable with my cobbled-together

Linux desktop, much more than just a few years ago. I think that as more

and more computing tasks become distributed - moved from the desktop to being powered by a central server - it

will become easier to rely on Linux on the desktop and the growth will continue.

-----

**Interview with Mitchell Rowton,**  
**[37]<http://www.securitydocs.com/>**

**Astalavista** : Hello Mitchell, would you please tell us something more about your background in the information security industry, and what is SecurityDocs.com all about?

**Mitchell** : I joined the US Marine Corps after high school. There I worked a helpdesk for a year or so before moving on to being a server administrator. After a while I became more and more interested in the networking side of things

(switches and routers.) Firewalls weren't used that often back then, and one day I was asked to put up an

access-control list (ACL) on our borderrouter. After that I started getting more and more security responsibility.

When I left the Marine Corps I used my security clearance to get a job as a DoD contractor, then a contractor in the health care industry.

By this time in my life I had a wife and kids. So I took a job that was more stable and didn't have as much travel

closer to home. When I think back, this is probably when the idea behind SecurityDocs.com was born. While I was

leaving one job and going to another I was told to do a very in depth turnover about starting an incident response

103

team at the company. So how do you explain how to start an incident response team at a fortune 500 company in a turnover document? After a while I gave up and put several dozen links to white papers that discuss starting an

incident response team.

Basically that's what SecurityDocs.com is - a collection of security white papers that are organized into categories so

that it's easy for someone to learn any particular area.

**Astalavista** : The media and a large number of privacy concious experts keep targeting Google and how unseriously

the company is taking the privacy concerns of its users. What is your opinion on that? Do you think a public

company such as Google should keep to its one-page privacy policy and contradictive statements given the fact that

it's the world's most popular

search engine?

**Mitchell** : I should start off by saying that my company makes money through Google's Adsense program. That being

said, it seems like most of the media hoopla surrounding Google privacy has centered around gmail and desktop

search. I just don't see a problem with either of these issues. I signed up for gmail knowing that I would see targeted

text ads based on the content of e-mail that I was viewing.

And I know that Google is going to learn some general stuff about everyones desktop searching habits. They will

know that pdf's are searched for more often than spreadsheets and other non-specific information. None of which

is personally identifiable.

**Astalavista** : Phishing attacks are on the rise, each and every month we see an increasing number of new emails

targeting new companies. What do you think of the recent exploit of the SunTrust bank web site? Are users really

falling victims to these attacks or even worse, they're getting even more scared to shop online?

**Mitchell** : The blame in this specific case falls mostly with the bank, but also on the users. I can't remember the last time my bank asked me for my atm or credit card number on a non-secure page. That being said, I know that my

grand mother would probably fall for this. Sure users should check for SSL Certificates and use common sense. But

more importantly financial institutions should not allow cross site scripting or malicious scripting injections.

If this type of phishing continues to rise then I imagine it will make the average user a little more worried about

giving information online. This is bad for companies, but as a security guy, I think that most users should be more

worried about who they give their information to. There are a lot of phishing attacks that have nothing to do with

the [38]institutions. In cases like this, users must use some basic security common sense or risk getting scammed.

**Astalavista** : What used to be a worm in wild launched by a 15 years old kid or hactivist, has recently turned into

"DDoS services on demand", what do you think made this possible? Is it the unemployed authors themselves, the

real criminals realizing the potential of the Internet, or the unethical competition?

**Mitchell** : I'm sure it's a combination of all three. But it's also getting more popular because it hurts more today than it used to. Five years ago an organizations web site was usually little more than an online brochure that wasn't too

important in the scheme of things. Today their website is probably tightly integrated into their business model, and

will cause a large financial and reputation loss if it is compromised or unusable.

The first step in doing a security assessment is to determine what's really important. Most companies should realize

that having the same security mechanisms in place that they had three years ago is putting them more and more at

risk because these security mechanisms are protecting information that gets more important every day.

**Astalavista** : Recently, the FBI has been questioning  
Fyodor, the author of NMAP over accessing server logs from

104

insecure.org. Do you think these actions, legal or not, can have any future implications on the users's privacy at other web sites? I mean, next it could be any site believed to be visited by a criminal, and besides all how useful this information might be in an investigation?

**Mitchell** : I had a mixed reaction when I first read about this. But I must say that Fyodor handled this superbly. He sent an e-mail out telling people what was happening and explaining that he was only complying with properly

served subpoenas. He also puts things into perspective. If someone hacks into a server and downloads nmap at a

specific time, then perhaps law enforcement should be able to view the nmap server logs for that specific time. On

the other hand what if I were also downloading NMap at that time? I personally wouldn't care if anyone knows that

I download nmap, but I can also understand why other people would be bothered by this. Overall I agree with very

narrow subpoenas directed at specific time periods and source IP's.

Technorati tags :

[39]Security, [40]Progenic, [41]Jason Scott, [42]Kevin Townsend, [43]Richard Menta, [44]Astalavista, [45]Candid

Wuest,

[46]Anthony Aykut, [47]David Wreski, [48]Mitchell Rowtow,  
[49]Björn Andreasson, [50]Dallas Con, [51]Nikolay

Nedyalkov, [52]Roman Polesek, [53]Cryptome, [54]Eric  
Goldman, [55]Johannes Ullrich, [56]Daniel Brandt,  
[57]David

Endler, [58]3APA3A

1. <http://www.astalavista.com/index.php?section=newsletter>
2. <http://ddanchev.blogspot.com/2006/01/security-interviews-20042005-part-2.html>
3. <http://ddanchev.blogspot.com/2006/01/security-interviews-20042005-part-3.html>
4. <http://www.progenic.com/>
5. <http://www.textfiles.com/>
6. <http://www.itsecurity.com/>
7. <http://www.bankinfosecurity.com/>
8. <https://draft.blogger.com/null>
9. <http://www.cyberarmy.net/>
10. <http://www.astalavista.com/>
11. <http://www.trojan.ch/>
12. <http://www.frame4.com/>
13. <http://www.linuxsecurity.com/>
14. <http://www.securitydocs.com/>

15. <http://www.snake-basket.de/>
16. <http://www.warindustries.com/>
17. <http://www.dallascon.com/>
18. <http://www.iseca.org/>
19. <http://www.hakin9.org/en/>
20. <http://www.cryptome.org/>
21. <http://www.ericgoldman.org/>
22. <http://www.cgisecurity.com/>
23. <http://isc.sans.org/>
24. <http://google-watch.org/>
25. <http://www.tippingpoint.com/>
26. <http://security.nnov.ru/>
27. <http://www.progenic.com/>
28. <http://www.textfiles.com/>
29. <http://www.itsecurity.com/>
30. <http://www.hicomm.bg/>
- 105
31. <http://bankinfosecurity.com/>
32. <http://www.cyberarmy.net/>
33. <http://www.astalavista.com/>



34. <http://www.trojan.ch/>
35. <http://www.frame4.com/>
36. <http://www.linuxsecurity.com/>
37. <http://www.securitydocs.com/>
38. [http://www.fraudwatchinternational.com/fraudalerts2/0412/pages/041207\\_4176\\_bankamerica.htm](http://www.fraudwatchinternational.com/fraudalerts2/0412/pages/041207_4176_bankamerica.htm)
39. <http://technorati.com/tag/Security>
40. <http://technorati.com/tag/Progenic>
41. <http://technorati.com/tag/Jason+Scott>
42. <http://technorati.com/tag/Kevin+Townsend>
43. <http://technorati.com/tag/Richard+Menta>
44. <http://technorati.com/tag/Astalavista>
45. <http://technorati.com/tag/Candid+Wuest>
46. <http://technorati.com/tag/Anthony+Aykut>
47. <http://technorati.com/tag/David+Wreski>
48. <http://technorati.com/tag/Mitchell+Rowtow>
49. <http://technorati.com/tag/Bj%C3%83%C2%B6rn+Andreasson>
50. <http://technorati.com/tag/Dallas+Con>

51. <http://technorati.com/tag/Nikolay+Nedyalkov>
52. <http://technorati.com/tag/Roman+Polesek>
53. <http://technorati.com/tag/Cryptome>
54. <http://technorati.com/tag/Eric+Goldman>
55. <http://technorati.com/tag/Johannes+Ullrich>
56. <http://technorati.com/tag/Daniel+Brandt>
57. <http://technorati.com/tag/David+Endler>
58. <http://technorati.com/tag/3APA3A>

106



## **Personal Data Security Breaches - 2000/2005 (2006-01-26 18:04)**

[1]

Another invaluable CRS report that I came across to, including detailed samples of all the

[2]data security breaches in between 2000 and 2005(excluding the ones not reported or still undergoing of course),

covering :

- The accident
- Data publicized
- Who was affected

- Number of affected
- Type of data compromised
- Source of the info

Here are some cases worth mentioning as well :

1. [3]Indiana University - malicious software programs installed on business instructor's computer, November, 2005
2. [4]University of Tennessee -inadvertent posting of names and Social Security numbers to Internet listserv, October, 2005
3. [5]Miami University (Ohio) - report containing SSNs and grades of more than 20,000 students has been accessible via the Internet since 2002, September, 2005
4. [6]Kent State University - five desktop computers stolen from campus, 100,000 people affected, September, 2005
5. [7]University of Connecticut -hacking - rootkit (collection of programs that a hacker uses to mask intrusion and obtain administrator-level access to a computer or computer network)placed on server on October 26,2003, but not detected until July 20, 2005

Quite a huge number of exposed people, and 20 % of the problem represents lost or stolen laptops or tapes,

the rest is direct hacking of course. It's impressive how easy is to get access to sensitive, both personal and financial information though what is already stored somewhere else in a huge and plain-text database for sure. And that

simply shouldn't be allowed to happen, or at least someone has to be held accountable for not taking care of the

confidentiality of the information stored.

Technorati tags :

[8]security,[9]information security,[10]id theft,[11]security breach,[12]security statistics

1. <https://web.archive.org/web/20101016193525/http://photos1.blogger.com/blogger/1933/1779/1600/idtheft.jpg>

2. [http://www.opencrs.com/rpts/RL33199\\_20051216.pdf](http://www.opencrs.com/rpts/RL33199_20051216.pdf)

3. <http://www.indiana.edu/>

4. <http://www.utk.edu/>

5. <http://www.miami.muohio.edu/>

6. <http://www.kent.edu/>

107

7. <http://www.uconn.edu/>

8. <http://technorati.com/tag/security>

9. <http://technorati.com/tag/information+security>

10. <http://technorati.com/tag/id+theft>

11. <http://technorati.com/tag/security+breach>

12. <http://technorati.com/tag/security+statistics>

108



### **Skype to control botnets?! (2006-01-26 18:13)**

[1]

I just read an article from CNET on how "[2]Skype could provide botnet controls",

with which I totally disagree. Skype and VoIP communications can actually provide [3]botnet herders with the oppor-

tunity to communicate, compared to acting as a platform for malicious attacks.

And old fashioned DDoS attacks the way we know them work damn well as a concept. Years ago, quite some :) linux

boxes worming was on the rise the [4]Honeynet Project was conducting [5]outstanding research to build awareness

on this fact. These days, with the penetration of broadband, and the thousands of users with ISP like bandwidth make

the need to look for bandwidth irrelevant. Instead of breaching into core routers and looking for bandwidth, that

DDoS attack power is gathered through the collective breaching of thousands of hundreds unprotected, unaware or

naive end users.

Botnet communications are evolving each time a new disrupting technology pops up, on the other hand, botnet

herders are having trouble in finding out the exact number of their botnet due to lack of server capacity, and as I've

once mentioned in my [6]Malware - future trends research, encryption seems to be the logical move.

And the trade off would eventually be the delays of communication given the size of the botnet and the encryption

approaches of course. Bots that lack the weakness of idleness on public IRC servers are already "talking" and trying to act as legit as possible, my point is that the bigger a botnet gets, the harder is to maintain it, that's logical, and it's good news for everyone, until someone standardize a possible communication protocol.

Scary thoughts, but a simple botnet/malware communication protocol could for instance cause a lot of troubles for

everyone. Is centralization of botnets a good thing for the industry in respect to tracking them, and how would things

evolve? Skype is totally out of the question from my point of view, or is it not?

Some nice insights on botnet communications can be found at :

[7]The Zombie Roundup: Understanding, Detecting, and Disrupting Botnets

Technorati tags :

[8]security,[9]information security,[10]malware,[11]botnets,  
[12]skype

1. <https://web.archive.org/web/20101016193525/http://photos1.blogger.com/blogger/1933/1779/1600/hacker.2.jpg>
2. [http://news.com.com/2100-7349\\_3-6031306.html](http://news.com.com/2100-7349_3-6031306.html)
3. <http://ddanchev.blogspot.com/2006/01/what-are-botnet-herds-up-to.html>
4. <http://www.honeynet.org/>
5. <http://www.honeynet.org/papers/kye.html>
6. <http://ddanchev.blogspot.com/2006/01/malware-future-trends.html>
7. [http://www.arbornetworks.com/downloads/research130/sruti05\\_final.pdf](http://www.arbornetworks.com/downloads/research130/sruti05_final.pdf)
8. <http://technorati.com/tag/security>
9. <http://technorati.com/tag/information+security>
10. <http://technorati.com/tag/malware>
11. <http://technorati.com/tag/botnets>

12. <http://technorati.com/tag/skype>

109

## **Security Interviews 2004/2005 - Part 3 (2006-01-26 18:46)**

Part 3 includes :

17. **Eric Goldman** - [1]<http://www.ericgoldman.org/> - 2005

18. **Robert** - [2]<http://www.cgisecurity.com/> - 2005

19. **Johannes B. Ullrich** - [3]<http://isc.sans.org/> - 2005

20. **Daniel Brandt** - [4]<http://google-watch.org/> - 2005

21. **David Endler** - [5]<http://www.tippingpoint.com/> - 2005

22. **Vladimir, ZARAZA** - [6]<http://security.nnov.ru/> - 2005

Go through [7]Part 1 and [8]Part 2 as well!

Part of [9]Asta's Security Newsletter

-----

**Interview with Eric Goldman,**  
[10]<http://www.ericgoldman.org/>

**Astalavista** : Hi Eric, would you, please, introduce yourself to our readers and share some info about your pro-

fession and experience in the industry?

**Eric** : I am an Assistant Professor of Law at [11]Marquette University Law School in Milwaukee, Wisconsin. I



have been a full-time professor for 3 years. Before becoming an academic, I was an Internet lawyer for 8 years in the Silicon Valley. I worked first at a private law firm, where most of my clients were Internet companies that allowed users to interact with other users (eBay was a leading example of that). Then, from 2000-2002, I worked at [12]Epinions.com (soon to be part of eBay) as its general counsel. As

an academic, I principally spend my time thinking and writing about Internet law topics. Some of my [13]recent papers have addressed warez trading, spam, search engine liability and adware. I run two blogs: [14]Technology & Marketing Law Blog, where we discuss many Internet law, IP law and marketing law topics, and [15]Goldman's Observations, a personal blog where I comment on other topics of interest.

**Astalavista** : Teaching tech and Internet-savvy students on CyberLaw and Copyrights infringement is definitely

a challenge when it comes to influencing attitudes, while perhaps creative when it comes to discussions. What's the overall attitude of your students towards online music and movies sharing?

**Eric** : Students have a variety of perspectives about file sharing. Some students come from a content owner

background; for example, they may have been a freelance author in the past. These students tend to strongly

support the enforcement efforts of content owners, and they view unpermitted file sharing as stealing/theft,

etc. Other students come from a technology background and subscribe to the “information wants to be free?”

philosophy. These students come into the classroom pretty hostile to content owners’ efforts and tend to be

fatalistic about the long-term success of enforcement efforts. However, I think both of these groups are the minority.

I think the significant majority of students do not really understand how copyright law applies to file sharing.

They learned how to share files in school and do so regularly without fully understanding the legal ramifications.

Usually, their thinking is: “if everyone is doing it, it must be OK.” These students tend to be surprised by the

incongruity between their behavior and the law. Even when we discuss the rather restrictive nature of copyright

law, these students are not always convinced to change their behavior. Deep down, they still want the files

they want, and file sharing is how they get those files. As a result, I’ll be interested to see how attitudes evolve

with the emergence of legal download sites like iTunes. I suspect these sites may be retraining students that there

is a cost-affordable (but not free) way to get the files they want. We’ll see how this changes the classroom discussions!

**Astalavista** : Where do you think is the weakest link when it comes to copyright infringement of content online, the distribution process of the content or its development practices?

**Eric** : With respect to activities like warez trading, consistently the weakest link has been insiders at content companies. Not surprisingly (at least to security professionals), employees are the biggest security risk. I do think

content owners are aware of these risks and have taken a number of steps to improve in-house security, but the

content owners will never be able to eliminate this risk. I'd like to note a second-order issue here. Content owners

have historically staggered the release of their content across different geographical markets. We've recently seen a

trend towards content owners releasing their content on the same day worldwide (the most recent Harry Potter book

is a good example of that). I think the content owners' global release of content will reduce some of the damage from

warez traders distributing content before it's been released in other geographic markets. So as the content owners

evolve their distribution practices, they will help limit the impact of other weak links in the distribution process.

**Astalavista** : Do you envision the commercialization of P2P networks given the amount of multimedia traded

there, and the obvious fact that Internet users are willing to spend money on online content purchases (given Apple's

Itune store success, even Shawn Fanning's Snocap for instance) given the potential of this technology?

**Eric** : Personally, I'm not optimistic about the commercialization of the P2P networks. The content owners

continue to show little interest in embracing the current forms of technology. I think if the content owners wanted

to go in this direction, they would have done so before spending years and lots of money litigating against Napster,

Aimster, Grokster and Streamcast.

In my opinion, without the buy-in of the content owners, P2P networks have little chance of becoming the

dominant form of commercialized content downloads. So I think, for now, we'll see much more content owners'

efforts directed towards proprietary download sites than cooperation with the P2P networks.

**Astalavista** : Were spyware/adware as well as malware the main influence factors for users to start legally

purchasing entertainment content online?

**Eric** : We have some evidence to suggest otherwise. A recent [16]study conducted at UC Berkeley watched

the behavior of users downloading file-sharing software. The users didn't understand the EULAs they were presented

with, so they were not very careful about downloading. But, more importantly, the users persisted in downloading

file-sharing software even when they were told and clearly understood that the software was bundled with adware.

If this result is believable, users will tolerate software bundles—even if those bundles are risky from a security

standpoint—so long as the software will help them get where they want.

Instead, I would attribute the comparative success of the music download sites to their responsiveness to con-

sumer needs. Consumers have made it clear what they want—they want music when they want it, they want to listen

to it in the order of their choosing, they want to pay a low amount for just the music they want (not the music they

don't), they want the interface to be user-friendly and they want to deal with trustworthy sources. Also, consumers

have surprisingly eclectic tastes, so any music download site must have a large database that's

diverse enough to satisfy idiosyncratic tastes. The most recent generation of music download sites have finally

provided an offering that satisfies most of these key attributes. They aren't perfect yet, but the modern sites are

so much better than prior offering where the pricing was off, the databases were incomplete, or the sites were still

trying to tell consumers how they should enjoy the music (rather than letting the consumers decide for themselves).

P2P file-sharing networks still serve a consumer need, but the content owners have succeeded some in in-

creasing the search costs that consumers have to receive (such as by using spoof files). As consumer search

costs using file-sharing increase, legal downloading sites with efficient search/navigation interfaces become more

111

attractive.

**Astalavista** : How would you explain the major investments of known companies

into spyware/adware? Is it legal but unethical from a moral point of view?

**Eric** : I'm a little contrarian on this topic, so I may be unintentionally controversial here. From my perspective, we should start with a basic proposition: adware and spyware are not inherently evil. Like many other technologies,

adware and spyware are good technology capable of being misused. Indeed, I think adware and spyware are an

essential part of our future technological toolkit—perhaps not in the existing form, but in some form. We should

not dismiss the technology any more than we should dismiss P2P file sharing technology simply because many users

choose to engage in illegal file sharing using it.

Once we realize that adware and spyware are not necessarily bad and could even be useful, then it makes

sense that major brand-name companies are working with adware/spyware. Adware and spyware offer new—and

potentially better—ways to solve consumers' needs, so we should expect and want companies to continue inno-

vating. Let me give an example. I use Microsoft XP and it constantly watches my activities. Indeed, in response to

my actions/inactions, I get lots of pop-up alerts/notifications....“updates are available? “you are now connected

online? “we have detected a virus? etc. I want my operating system to be monitoring my behavior and alerting me

to problems that need my attention. In fact, I'd be happy if Microsoft fixed problems that don't need my attention

without even disturbing me. Microsoft is aware of this and is working on technological [17]innovations to be smarter

about when it delivers alerts.

So from my perspective, Microsoft is in the spyware business. They have huge investments in spyware. I'm

glad they are making these investments and I hope they find even better ways to implement their software. I think

adware and spyware have been maligned because a number of otherwise-legitimate marketers have engaged in (and

may continue to engage in) some questionable practices. These practices can range from deceptive/ambiguous dis-

closures to exploiting security holes. I remain optimistic that legitimate businesses will evolve their practices. We've seen

movement by companies like Claria (eliminating pop-up ads), WhenU (deliberately scaling back installations by taking more efforts to confirm that users want the software) and 180solutions (cleaning up its distribution channels).

This is not to say that we've reached the right place yet, but I like to think that the major adware companies will continue to improve their practices over time.

However, there will also be people who will disseminate software that is intended to harm consumers, such

as by destroying or stealing data. We have to remain constantly vigilant against these threats. But they are far from

new; we've had to deal with malicious virus writers for a couple of decades. In thinking about the policy implications,

we should not lump the purveyors of intentionally harmful software together with legitimate businesses that are

evolving their business practices.

**Astalavista** : Do you think the distributed and globalized nature of the Internet is actually the double edged

sword when it comes to fighting/tracing cyber criminals and limiting the impact of an already distributed/hosted

copyrighted information?

**Eric** : There's no question that the global nature of the Internet poses significant challenges to enforcement



against infringement and criminals. While this is mostly a problem, the need for cross-border coordination creates

an opportunity for governments to develop compatible laws and legal systems, and there could be real long-term

benefits from that.

**Astalavista** : What's your opinion on the current state of DRM (Digital Rights Management) when it comes to

usefulness and global acceptance?

112

**Eric** : I know DRM is pretty unpopular in a lot of circles, especially academic circles. Personally, I don't have a problem with DRM. I look at DRM as a way of determining the attributes of the product I'm buying. Consider the

analogy to physical space. When I buy a car, most manufacturers give me some options to purchase. For example,

I can upgrade the seat covers to the leather package if I'm willing to pay for that. The manufacturer could make

that choice for me (and sometimes they do), but when it's my choice, I can pay for what I value. DRM is a way of

creating different product attributes in digital bits. In theory, with DRM, I can buy 24 hour viewing rights, 1 year

viewing rights or perpetual viewing rights. Depending on my needs, I may prefer to pay less and get less, or I may

want the perpetual rights and will happily pay more for that. Without DRM, we've relied on physical nature of the

content storage medium, plus post-hoc copyright infringement enforcement, to establish those different attributes.

DRM does a much more effective job of defining the product. Therefore, DRM gives the content owners new ways

to create products that respond to consumer needs. Of course, consumers need to understand what they are buying

when it's controlled by DRM, but that's a consumer disclosure issue that we've encountered in lots of contexts before.

As far as I can tell, consumers have no problem with DRM. Indeed, the comparative success of download sites

like iTunes indicates that consumers don't really care about DRM so long as they can get what they want.

**Astalavista** : In conclusion, I would really appreciate if you share your comments

about the Astalavista.com site and, particularly, about our security newsletter?

**Eric** : My first introduction to your site was when one of my articles was linked on the site. My traffic immedi-

ately took off like a rocket ship. I was very impressed with the quantity and

sophistication of your readers. Thanks for giving me an opportunity to speak with them.

-----

**Interview with Robert,**  
[18]<http://www.cgisecurity.com/>

**Astalavista** : Hi Robert, would you, please, introduce yourself to our readers and share some info about your profession and experience in the industry?

**Robert** : I first started to get interested in the hacker/security aspect of computers in the 90's in high school

where I had my first brush with a non 'windows/mac system' called 'VMS' (a VAX/VMS system to be exact). A

year later I \*finally\* got access to an internet connection and to my amazement discovered that it was possible to

break into a website with nothing more than your browser which was something I found to be rather interesting.

This \*interest\* grew into a website I originally hosted on xoom (some free hoster I forget which :) that later became

CGISecurity.com in September of 2000 where I've published numerous articles and white papers pertaining to

website security. In 2003 I 'sold out' (get paid to do what you'd do for free ) and was hired to perform R &D; and

QA on a Web Application Security Product where I am to this day. In 2004 I Co Founded [19]'The Web Application

Security Consortium' with [20]Jeremiah Grossman to provide an outlet for some projects that multiple people we

knew were interested in participating in. A year later I created [21]'The Web Security Mailing List' as a forum where

people can freely discuss all aspects of Web Security where I am currently the lead list moderator.

**Astalavista** : Recently, there's been a growing trend towards the use of automated code auditing/exploitation

tools in web applications security. Do you believe automation in this particular case gives a false sense of security,

and provides managers with point'n'click efficiency, compared to a structured and an in-depth approach from a consultant?

**Robert** : Scanners provide a good baseline of the common types of issues that exist but are not magic bullets.

It shouldn't come to a surprise to you but many of these consultants use these automated scanning tools (Both

freeware and commercial) in conjunction with manual review and simply verify the results. The skill of the person

using any specialized product greatly impacts the end result. Someone with a good security understanding can save

113

immense amounts of time by using such an automated product. If your organization doesn't have a 'security guy'

then a consultant may be the best solution for you.

**Astalavista** : Phishers are indeed taking a large portion of today's e-commerce flow. Do you believe corpora-

tions are greatly contributing to the epidemic, by not taking web security seriously enough to ensure their web sites

aren't vulnerable to attacks in favour of online scammers?

**Robert** : Phishing doesn't \*require\* that a website be vulnerable to anything it just simply requires a look

alike site exploiting a users lack of security education and/or patches. I wouldn't say they are contributing towards it, but I do think that educating your user (as best as you can)

is a requirement that should be in place at any online organization.

**Astalavista** : What are you comments on the future use of web application worms, compared to today's bot-

nets/scams oriented malware? What are the opportunities and how do you picture their potential/use in the

upcoming future?

**Robert** : In 2005 we saw a rise in the use of search engines to 'data mine' Vulnerable and/or suspect hosts.

Some of the larger search engines are starting to put measures in place such as daily request limitations, CAPTCHA's,

and string filtering to help slow down the issue. While these efforts are noteworthy they are not going to be able to

prevent \*all\* malicious uses

a search engine allows. I think the future 'web worms' will borrow methodologies from security scanners created to

discover new vulnerabilities that will have no patches available. While the downside of this is to slow infection rates

and lots of noise, the upside is infecting machines with no vendor supplied patch available because the 'vendor' may be a consultant or ex employee who is no longer available. Worms such as Nimda infected both the server and its

visitors making it highly effective and I expect this user/server trend to increase in the future. I also suspect a switch towards 'data mining' worms, that is worms that are trying to steal useful data. Modern day versions of these worms

steal cd keys to games and operating systems. The use

of worms to seek and steal data from a server environment, or user machine is only going to grow as credit card and

identity theft continue to grow. While investigating a break-in into a friends ISP I discovered the use of a shopping

cart 'kit' left behind by the attacker. This kit contained roughly 8 popular online shopping carts that where modified

to grab copies of a customers order, a 'shopping cart rootkit' if you will. I suspect some type of automation of either

auto backdooring of popular software or uploading modified copies to start creeping its way into future web worms.

In 2002 I wrote an article titled [22]'Anatomy of the web application worm' describing some of these 'new' threats

that web application worms maybring to us.

**Astalavista** : Is the multitude and availability of open-source or freeware web application exploitation tools

benefiting the industry, resulting in constant abuse of web servers worldwide, or actually making the situation even

worse for the still catching up corporations given the overall web applications abuse?

**Robert** : This entirely depends on the 'product'. There are tools that allow you to verify if a host is vulnerable without actually exploiting it which I consider to be a good thing while some of these 'point and root' tools are not

helping out as many people as they are hurting. In the past

few years a shift has started involving 'full disclosure' where people are deciding not to release ./hack friendly ex-

ploits but are instead releasing 'just enough detail' for someone to verify it. This 'shift' is something that I fully support.

**Astalavista** : CGISecurity.com has been around for quite a few years. What are your plans for future projects

regarding web security, and is it that you feel the industry is lacking right now - awareness, capabilities or incentives to deal with the problem?

**Robert** : Actually September 14th will be the 5th year anniversary of CGISecurity.com. Right now I'm heavily

114

involved in 'The Web Application Security Consortium' where we have numerous projects underway to provide

documentation, education, and guides for users. I plan on expanding CGI Security into a one stop shop for all 'web

security' related documentation where you can (hopefully) find just about anything you could ever need. To answer

the second part of your question I'd say all three with awareness (education) being the biggest problem.

One of the things that the industry hasn't 'gotten' yet (in my opinion) is security review throughout an application's

lifecycle. Sure developers are starting to take 'secure development' more seriously but as many of your readers know

deadlines hamper good intentions and often temporary solutions (if at all) are put in place to make something work

in time for release. This is why we need security review during all phases of the cycle not just during development

and post production. I think that a much overlooked aspect of the development cycle is Quality Assurance. QA's job

is to ensure that a product works according to requirements, identify as many pre release (and post release) bugs

as possible, and to think about ways to break the product. I think that more companies need to implement 'QA

security testing' as a release requirement as well as train their testers to have a deeper understanding of these 'bugs'

that they've been discovering. You've heard the term 'security in layers' so why can't this process be implemented



throughout most development cycles? Developers get busy and may overlook something in the rush to meet the

release date which is why (before release)

they need someone double checking their work (QA) before it goes production.

**Astalavista** : In conclusion, I would like to ask you what is your opinion of the Astalavista.com's web site and,

in particular, our security newsletter?

**Robert** : I first discovered astalavista in my 'referrer' logs when it linked to one of my articles. Since then I've been visiting on and off for a few years and only recently discovered the newsletter which I think is a great resource

for those unable to keep up with all the news sites, and mailing list postings.

-----

**Interview with David Endler,**  
[23]<http://www.tippingpoint.com/>

**Astalavista** : Hi Dave, would you, please, introduce yourself to our readers and share with us some info about your experience in the industry?

**Dave** : Sure, I'm 6'1", a Leo, I like long walks on the beach, coffee ice cream, ^H^H^H^H^H^H^H . . . oh,

sorry, wrong window. I'm the Director of Security Research at 3Com's security division, TippingPoint. Some of

the functions that fall under me include 3Com's internal product Security testing, 3Com Security Response, and the Digital Vaccine team Responsible for TippingPoint IPS vulnerability filters. Prior to 3Com, I was the director of iDefense Labs overseeing vulnerability and malware research. Before that, I had various security research roles with

Xerox Corporation, the National Security Agency, and MIT.

**Astalavista** : What's the goal of your Zero Day Initiative, how successful is your approach so far, and what differentiates it from iDefense's one?

**Dave** : Over the past few years, no one can deny the obvious increase in the number of capable security researchers as well as the advancement of publicly available security researching tools. We wanted to tap into this network of global researchers in such a manner as to benefit the researchers, 3Com customers, and the general public. Our approach was the construction of the [24]Zero Day Initiative (ZDI), , launched on August 15, 2005. The main goals behind the program are:

**a.)** Extend 3Com's existing vulnerability research organization by leveraging

the methodologies, expertise, and time of others.

**b.)** Responsibly report 0day vulnerabilities to the affected vendors

**c.)** Protect our customers through the TippingPoint Intrusion Prevention Systems (IPS) while the product vendor is working on a patch

**d.)** Protect all technology end users by eliminating 0day vulnerabilities

through collaboration with the security community, both vendors and

researchers.

The ZDI has had an incredibly positive result in only three months of activity, far exceeding our expectations.

To date we have had over 200 researchers sign up through the portal, and received over 100 vulnerability submis-

sions. We suspect that part of the early success of the program can be attributed to the wild launch party we threw at [25]Blackhat/Defcon 2005.

The ZDI is different from iDefense's program in a number of ways. 3Com has invested considerable resources

to ensure the success of the ZDI. As a result, ZDI contributors will receive a much higher valuation for their research.

We provide 0day protection filters for our clients, without disclosing any details regarding the vulnerability, through

our TippingPoint IPS, as opposed to simply selling vulnerability details in advance of public disclosure. Finally,

we

altruistically attempt to protect the public at large by sharing the acquired 0day data with other security vendors (yes, this includes competitors) in an effort to do the most good with the information we have acquired. We feel we can

still maintain a competitive advantage with respect to our customers while facilitating the protection of a customer

base larger than our own.

**Astalavista** : 0day vulnerabilities have always been a buzzword in the security community, while in recent

years decision makers have started realizing their importance when evaluating possible solutions as well. What's the

myth behind 0day vulnerabilities from your point of view,

and should it get the highest priority the way I'm seeing it recently?

**Dave** : Certainly not all vulnerabilities should be treated equally, including 0day. A typical vendor-announced

vulnerability can be just as devastating as a 0day due to the trend of shrinking windows of time for exploit release.

Obviously, for an organization or home user that doesn't stay up-to-date with security patches, a three-year old

exploit for a patched vulnerability could be just as devastating as a 0day exploit. I think 0day vulnerability protection has begun to take more shape in security buying

decisions simply due to the growing frustration and helplessness

felt by users when vendors take a long time to patch these issues when exploits are widely circulating. In the last year alone, we saw several of the 0day browser exploits incorporated into spyware sites within one day of their disclosure.

**Astalavista** : Do you feel the ongoing monetization and actual development of security vulnerabilities market

would act as an incentive for a ShadowCrew style underground market, whose "rewards" for 0day vulnerabilities will contribute to its instant monopoly?

**Dave** : I think there will always be an underground market, but I doubt it will ever have a monopoly for a few

reasons. We know there is a thriving underground market today for 0days, especially browser vulnerabilities that

can be used to inject Trojans and steal financial data. I think the main obstacle currently curbing the growth of the

underground vulnerability-purchase

movement is a lack of trust. Since a security researcher doesn't really know the identity of an underground buyer,

there's no guarantee he will get paid once he unveils his discovery. Also at the end of the day, many researchers

want these vulnerabilities to be fixed and want to receive the appropriate recognition in the mainstream security

community.

**Astalavista** : While you are currently acting as the intermediary between a vendor and researcher, do you picture the long-term scenario of actually bidding for someone else's research given the appearance of other competitors, the existence of the underground market I already mentioned, and the transparency of both? How do you think would the market evolve?

116

**Dave** : Good question. I hope the markets evolve in a way that encourages Vendors to put more skin in the game. It behooves these vendors to help protect their own customers more by rewarding outside researchers for

security discoveries that escape internal QA testing. The only vendors I know of who currently do this are Netscape and Mozilla through their bug bounty

programs. I think a "0-bay" auction model could be viable if a neutral party launched it that was trustworthy as a vulnerability "escrow agent" and could guarantee anonymity and payment to researchers. There was some good

discussion on the [26]Daily Dave list of some of the issues raised by such an auction model.

**Astalavista** : Should a vendor's competencies be judged on how promptly it reacts to a vulnerability notifica-

tion and actually provides a (working) fix? Moreover, should vendors be held somehow accountable for their

practices in situations like these, thus eliminating or opening up windows of opportunity for pretty much anything

malicious?

**Dave** : I've worn the hat of a security researcher, vulnerability disclosure intermediary, and most recently, a

vendor. I now have a great amount of sympathy for all three groups. In general, vendors need to make a more

concerted effort to reach out to security researchers in the vulnerability disclosure process. Many vendors don't

seem to understand that most security researchers get no tangible benefit for reporting a security issue. More

and more 0day disclosures it seems are also the result of a vendor-researcher relationship breaking down due

to a misunderstanding over email or poor follow-up from the vendor. Ideally, vendors should also reward these

researchers, if not with money, then other perks or recognition as a sign of appreciation. It's hard to judge all vendors the same on the amount of time it takes to patch a vulnerability. Some vulnerabilities legitimately take longer to fix

and QA than others. Because there are no laws today that govern a vendor's security response, the market is going

to have to be the ultimate judge in this arena. If enough potential customers are lost to a competitor because of poor

security patch handling or a destructive worm, you can bet that more money will be budgeted into their security

development lifecycle.

**Astalavista** : Having conducted security research for the NSA must have been quite an experience. Does the

agency's approach on security research somehow differ from the industry's one, in terms of needs for sure, but in

what way exactly?

**Dave** : No comment :-)

**Astalavista** : Can money buy creativity and innovation from an R &D's point of view?

**Dave** : Of course no amount of money can buy your way to really innovative research. Some of the most prolific

research teams are built through visionary research directors creating a nurturing and non-restrictive environment,

insulating the team from most corporate pressures and politics.

**Astalavista** : Thanks for your time!

-----

**Interview with Vladimir, aka 3APA3A**  
[27]<http://www.security.nnov.ru/>

**Astalavista** : Hi Vladimir, would you please introduce yourself to our readers, and share some info on your

background and experience with information security?



**Vladimir** : OK. I'm 31, I'm married, and we have two daughters. For last 10 years I'm support service head for middle sized ISP in Nizhny Novgorod, Russia. As so, I'm not occupied in IT security industry and I'm not security professional. It's just a kind of useful hobby. And that's the reason why I use nickname though I have no relation to

117

any illegal activity. Everyone who is interested can easily find my real name. In addition to my primary job, I give few classes a week on computer science in Nizhny Novgorod State University.

I started on the Russian scene in the late 90s with the article on HTTP chats security. 'Cross site scripting' was

quite new vulnerability class and the term itself arrived few years after. Later I began to publish some articles on

the Bugtraq. Because my previous nickname taken from Pushkin's personage was not understandable abroad, I used

gamer's nick '3APA3A', 'zaraza' in Cyrillic, it means infection. It also has a meaning of English 'swine' :). No, there is no relation with famous 3APA3A. ZARAZA virus, it was few years before.

I'm not 'bug digger', as one may think. Some bugs were discovered in the process of troubleshooting, while

others were found in attempt to discover new vulnerability class or exploitation approach. And I'm proud to catch a

few :)

**Astalavista** : What are some of your current and future projects?

**Vladimir** : Since 1999 [28]<http://www.security.nnov.ru>

is the only project I'm constantly involved in. Sometimes, I patch old bugs and create new ones within 3proxy

[29]<http://www.security.nnov.ru/soft/3proxy/> .

**Astalavista** : How would you describe the current state of the Russian security scene? Also, what are you

comments on the overall bad PR for, both, Russia, and Eastern Europe as a hackers' haven?

**Vladimir** : "hack" is an opposite to technology for me. The industry with technology is a conveyor, while the hack works only here and now. Hacking is the process of creating something to solve one particular problem without

enough money, resources and, most important, without knowledge. In the best case it's something new for everyone

and nobody to share knowledge and resources with you.

If you mean a lack of money, resources and knowledge - yes, Russia is hackers' heaven :)

We had interesting discussion on this topic with David Endler (from your Newsletter #23) Of cause you know

how many viruses originated from Russia and you know some "famous" virus writing teams. Do you know any

software written here? Well.. may be after some research you can find Outpost and Kaspersky Antivirus you have

never used... That's all. You think. Lets look at the city I live. Many really interesting things from Quake II graphical drivers and Intel debugging and profiling tools to Motorola and Nortel firmware were written here. It's not largest

city and Russia is large country. Same goes to Eastern Europe, India and China.

We have a lot of unknown programmers and few famous virus writers, that's the problem :)

The security scene in Russia is really hard question.

Of course, there are few professionals, they are well-

known buddies, who work for well-known companies. They publish their really useful books and write their really

professional articles and receive their really good money. There are old-school hackers who do not speak Russian for

few years. There are "underground" e-zines, none of them are living enough to spell correctly. There are "security teams" known by defacing each over and publishing up to 6 bugs in PHP scripts. Teenage #hax0r1ng IRC channels.

And, of cause, guys who do their business with trojans and botnets and prefer to stay invisible.

That's all, folks. There is no scene. No place to meet each over. No Russian Defcon.

**Astalavista** : What are the most significant trends that happened with vulnerability researching as a whole

since you've started your project?

**Vladimir** : Any new technology arrives as a hack, but grows into industry. It was with computers, software, network security and finally it happens with vulnerability research. This fact changes everything. No place left for

real hacking. The guys on this scene became professionals. If you enter this without knowledge, all you can is to find some bugs in unknown PHP scripts.

**Astalavista** : Do you think a huge percentage of today's Internet threats are mainly posed by the great deal of

window of vulnerabilities out there, and how should we respond to the concept of 0day by itself? Patching is

definitely not worth it on certain occasions from my point of view!

**Vladimir** : Imagine a 100,000,000 of purely patched default configuration Fedora Core machines with users

running their Mozilla's from root account. That's what we have in Windows world. Did you know that, 99 % of

Windows trojans/viruses/backdoors will not work if executed from unprivileged account? Life could be much more

secure if only administrator with special license (like driver's one) might configure system and get penalties in case

of virus incidents :)

Did you know that, most ISPs do not monitor suspicious activity from their customers and can not stop attack

from their network within 24 hours? It's almost impossible to coordinate something between providers. There are

non-formal organizations, like NSP-SEC, but it only coordinates large providers from few countries. Coordination and short abuse response time would be another step.

**Astalavista** : What is your attitude towards an 0day market for software vulnerabilities? And who wins and who loses from your point of view?

**Vladimir** : On the real market both sides win. No doubt, the fact there is now a legal market for 0days is a good news for researches and end users, because it rises vulnerability price and establishes some standards. This "white" market is in it's beginning. There are only few players.

Who can value 0day Internet Explorer bug? First of all, Microsoft. But for some reason it does not. The second, IDS/IPS vendors and security consulting companies to make signatures and PR. Bugtraq posting is really good PR. If vulnerability is then exploited in-the-wild, it raises the article in Washington Post. It's even better PR.

**Astalavista** : Do you also, somehow picture a centralized underground ecosystem, the way we are currently seeing/intercepting exchange of 0day vulnerabilities on IRC channels, web forums. But one with better transparency of its content, sellers and buyers?

**Vladimir** : And, of course, underground market is always ready to pay. Exploits are required to install a trojan.

Trojan is required to create a botnet. Botnet is required for spamming, DDoS and blackmailing, phishing, illegal

content hosting. It's definitely a kind of ecosystem with different roles and specializations and it's money cycle as a basement.

With some dirty games with 0day Internet Explorer vulnerability you can make a new car on the botnet mar-

ket or (and?) just few thousands dollars with PR. Underground market is not

centralized and lies on private contacts. Forums and IRC channels you can find are the top of the iceberg. It makes it less vulnerable. I bet last WMF exploit was sold without any IRC channels and forums.

**Astalavista** : Can there ever be a responsible disclosure, and how do you picture it?

**Vladimir** : According to Russian legislation, a vendor may not sell product without informing customer about

any known defect or imitation on it. I bet different countries have similar legislations. I don't understand why it

119

doesn't work with computer software. Vendor should either timely inform customers on defect in software or should stop to sell it.

Of course, disclosing information without informing vendor is just stupid and non-profitable for everyone. From other

side, a vendor has not eliminated vulnerability after few months and has

not informed customers there is nothing non-responsible in publishing this information. I never saw vendor who

blames researchers in non-responsible disclosure to stop selling defective product.

There were few attempts to standardize disclosure policy, FPolicy is the first one.

**Astalavista** : Can a vulnerability researcher gets evil if not treated properly, and what could follow? :)

**Vladimir** : Sure. Imagine a situation you want to get money from vendor for vulnerability information you dis-

covered. There is nothing bad in getting money for your work and

vendor should be interested in buying this information on the first place. But it can be just a blackmail if not "treated properly".

**Astalavista** : In conclusion, I wanted to ask on some of your future predictions for 2006 concerning vulnerabil-

ity research, and the industry as a whole?

**Vladimir** : One year is small period. Maybe we will see vendors to buy vulnerabilities. "Vulnerability researcher" may be scripted on somebody's business card and become

profession by this way. "Vulnerability researching" as University course... No, let's wait for another 2-3 years :)

**Astalavista** : Thank you for your time!

1. <http://www.ericgoldman.org/>
2. <http://www.cgisecurity.com/>
3. <http://isc.sans.org/>
4. <http://google-watch.org/>
5. <http://www.tippingpoint.com/>
6. <http://security.nnov.ru/>
7. <http://ddanchev.blogspot.com/2006/01/security-interviews-20042005-part-1.html>
8. <http://ddanchev.blogspot.com/2006/01/security-interviews-20042005-part-2.html>
9. <http://www.astalavista.com/index.php?section=newsletter>
10. <http://www.ericgoldman.org/>
11. <http://law.marquette.edu/cgi-bin/site.pl>
12. <http://www.epinions.com/>
13. [http://papers.ssrn.com/sol3/cf\\_dev/AbsByAuth.cfm?per\\_id=332758](http://papers.ssrn.com/sol3/cf_dev/AbsByAuth.cfm?per_id=332758)
14. <http://blog.ericgoldman.org/>
15. <http://blog.ericgoldman.org/personal>



16. [http://www.sims.berkeley.edu/~jensg/research/paper/grossklags-spyware\\_study.pdf](http://www.sims.berkeley.edu/~jensg/research/paper/grossklags-spyware_study.pdf)
17. <http://research.microsoft.com/~horvitz/attend.htm>
18. <http://www.cgisecurity.com/>
19. <http://www.webappsec.org/>
20. <http://www.whitehatsec.com/>
21. <http://www.webappsec.org/lists/websecurity/>
22. <http://www.cgisecurity.com/articles/worms.shtml>
23. <http://www.tippingpoint.com/>
24. <http://www.zerodayinitiative.com/>

120

25. [http://www.zerodayinitiative.com/party\\_2005/](http://www.zerodayinitiative.com/party_2005/)
26. <http://archives.neohapsis.com/archives/dailydave/2005-q2/0308.html>
27. <http://www.security.nnov.ru/>
28. <http://www.security.nnov.ru/>
29. <http://www.security.nnov.ru/soft/3proxy/>

121

**Security Interviews 2004/2005 - Part 2 (2006-01-26 19:31)**

Part 2 includes :

11. **Eric (SnakeByte)** - [1]<http://www.snake-basket.de/> - 2005

12. **Björn Andreasson** - [2]<http://www.warindustries.com/> - 2005

13. **Bruce** - [3]<http://www.dallascon.com/> - 2005

14. **Nikolay Nedyalkov** - [4]<http://www.iseca.org/> - 2005

15. **Roman Polesek** - [5]<http://www.hakin9.org/en/> - 2005

16. **John Young** - [6]<http://www.cryptome.org/> - 2005

Go through [7]Part 1 and [8]Part 3 as well!

[9]Part of Asta's Security Newsletter-----

**Interview with SnakeByte (Eric),**  
[10]<http://www.snake-basket.de/>

**Astalavista** : Hi Eric, would you please introduce yourself to our readers and share your experience in the security scene?

**Eric** : I am 24 years old, currently studying computer science in Darmstadt, Germany for quite some time now.

I am mostly a lazy guy, doing whatever I am currently interested in. My interest in computer security started with viruses ( no, I never spreaded one ), which were really interesting back then, but nowadays every worm looks the same;(

**Astalavista** : Things have changed much since the days of Webfringe, Progenic, BlackCode etc. What do you

think are the main threats to security these days? Is it our dependence on technologies and the Internet the fact that

it's insecure by design or you might have something else in mind?

**Eric** : I think security itself got a lot better since then but we have more dumb users who work hard to make

it worse now. Most users nowadays get flooded with viruses and just click them,

also the recent rise in phishing attacks - it's not the box which gets attacked here, it's the user. Security also got a lot more commercial.

**Astalavista** : What is your opinion on today's malware and virii scene? Do you think that groups such as the

infamous A29 have been gaining too much publicity? What do you think motivates virii writers and virii groups now

in comparison to a couple of years ago?

**Eric** : It's 29a :) And they deserve the publicity they got. They did and are doing some really cool stuff. But

they also were clever enough to be responsible with the stuff they created. About motivation for virii writers - it's

122

different for each of them, have to ask them.

But I think there is a new motivation - money. Nowadays you can get paid for a couple of infected computers, so spammers can abuse them.

**Astalavista** : What do you think of Symantec ? Is too much purchasing power under one roof going to end up

badly, or eventually the whole industry is going to benefit from their actions?

**Eric** : Sure monopolies are always bad but we get them everywhere nowadays. Maybe we need another revolution...

**Astalavista** : Is the practice of employing teen virii writers possessing what is thought to be a "know-how" a wise idea? Or it just promotes lack of law enforcement and creates ordes of source modifying or real malware coders?

**Eric** : I dont think it is a wise idea at all, but don't tell my boss ;-) Whether one has written virii or not should not influence your decision to you hire him/her.

**Astalavista** : Application security has gained much attention lately.

Since you have significant programming

experience, what do you think would be the trends in this field over the next couple of years, would software be indeed coded more securely?

**Eric** : Maybe,if universities started to teach coding in a secure way instead of teaching us more java bullcrap.

But I think the open source development is indeed helpful there. If you want to

run something like a server, a quick glance at the code will tell you whether you really want to use this piece or

search for another one.

**Astalavista** : Microsoft and its efforts to fight spyware has sparckled a huge debate over the Internet. Do you

think it's somehow ironic that MS's IE is the number one reason for the existence of spyware. Would we see yet

another industry build on MS's insecurities?

**Eric** : It's the only reasonable way for MS to react. Heh, they are just a company.

**Astalavista** : The Googlemania is still pretty hot. Are you somehow concerned about their one-page privacy

policy, contradictive statements, and the lack of retention policies given the fact that they process the world's

searches in the most advanced way and the U.S post 9/11 Internet wiretapping initiatives?

**Eric** : Yes I am, that's why their only product I use is the websearch function. As soon as I find another good

website like google.

**Astalavista**: Thanks for your time Eric!

-----  
Interview with Bjorn Andreasson,  
[11]<http://www.warindustries.com/>

**Astalavista** : Hi Bjorn, would you please introduce yourself and share some more information about your background in the security world?

**Bjorn** : My name is Bjorn "phonic" Andreasson and I live in Sweden, I'm turning 22 this year. I've been a part of the so called "underground" since the age of 14 which gives a total of 8 years. I got my first computer at the age 123

of 13 and I quickly got involved in Warez as my uncle showed me some basic stuff about the internet. After a while I realised Warez websites was "uncool" because of all the popups, porn ads, only trying to get as many clicks on your ads as possible to earn enough money to cover your phone bill. So, there I was viewing the Fringe of the web

([www.webfringe.com](http://www.webfringe.com)) and I found all those wonderful h/p/v/c/a websites, which caught my eye. I knew I could do

better than most of these guys as I had a lot of experience from the Warez scene -I knew how to attract visitors

quickly. The first version of War Industries I believe was a total ripoff from Warforge.com as I didn't know better at

the age of 15/16, I quickly understood this wasn't the way to do it so I made my first version of the War Industries

and I might add it looked VERY ugly as I recall it:)

From there I have had several designers making new versions, trying to improve it and I believe we've achieved that goal now. It should be mentioned that during 2000 and 2003 War Industries was put on ice as I couldn't cover the expenses so it was only me and a friend keeping the name alive until 2003 when I relaunched the website and turned it into what it is today (Badass). I've also been a part of the Progenic.com crew as well. As Blackcode.com crew, it was practically my work that made BC famous because I sent a shitload of hits to it back in '99 when WarIndustries received 4,000 unique hits on a daily basis. I also owned [www.icqwar.com](http://www.icqwar.com) which held only ICQ war tools, some of my own creation, very basic but handy. The site had 3,000 unique hits on a daily basis after only one week online. After four weeks I got a letter from AOL to give me the domain name or being sued. What could I do? 16 years old, of course, I gave it away! Well that's pretty much my story.

**Astalavista** : WarIndustries.com has been around since 1998, nice to see that it's still alive.

What is the site's mission, is it hacking or security oriented? Shall we expect some quality stuff to be released in the future, too?

**Bjorn** : WarIndustries can't really be placed anywhere. It's either black, gray or white hat. I'd say we're a mix

with a touch of them all. Our focus is to enlighten people in the means of programming, getting them to know google

as their best friend. We've released a couple of video tutorials which are very popular because they make things so easy. We're going to release a

couple of new ones soon, as soon as we get around to it as most of us got jobs and other stuff to attend to. Don't

miss out on our brand new T-shirts coming up in a month! If you're something, you've got to have one of those!

**Astalavista** : What do you think has changed during all these years? Give a comparison between the scene

back in 1998 as you knew it and today's global security industry, and is there a scene to talk about?

**Bjorn** : I'd say people are a way more enlightened today. Back in '98 you could pretty much do anything you

liked without getting caught. Today you can't even download Warez without getting problems. I'd say there's a scene

but very different from the oldschool I know. I am trying not to get involved and I have my own way. Maybe that's

why WarIndustries is so popular.

**Astalavista** : Is Google evil, or let's put it this way, how can Google be evil? Why would Google want to be

evil and what can we do about it if it starts getting too evil?

**Bjorn** : Google is not evil, Google is your best friend!

**Astalavista** : Give your comments on Microsoft's security ambitions given the fact that they've recently started



competing in the anti-virus industry. They even introduced anti-spyware application - all this coming from MS?

**Bjorn** : If it wasn't for Microsoft, there wouldn't be viruses so I'm blaming them for writing crap software.

Why do they always leave a project unfinished and start another one? I mean Windows XP is working fine, why

Longhorn? Why can't they make XP totally secure, like OpenBSD, there hasn't been a remote root exploit for many

years as of what I've heard? That's security! If I didn't know better, I'd say MS is writing low-quality software so they 124

can get

into the Anti-virus scene and make even more profits!

**Astalavista** : Recently, the EU has been actively debating software patents. Share your thoughts on this and

the future of open-source software?

**Bjorn** : I can't make up my mind when it comes to Open/Closed source. There's benefits from both sides. Open source is fixed much quicker but also discovered way more often than closed. This is my opinion.

**Astalavista** : In conclusion, I would really appreciate if you share your comments about the Astalavista.com

site and, particularly, about our security newsletter?

**Bjorn** : Actually, I haven't checked out Astalavista that much. I have known it for many years but I never got

around. I promise I'll check it out!

**Astalavista** : Thanks for your time **Bjorn**!

-----

**Interview with Bruce**, [12]<http://www.dallascon.com/>

**Astalavista** : Hi Bruce, would you please share with us some more information on your background in the security industry and what is DallasCon 2005 all about?

**Bruce** : Thanks for this opportunity. I have over 7 years of engineering experience working as a System's Engineer for companies such as Nortel Networks and Fujitsu. Realizing the importance of real information security training experience for everyday people, about 4 years ago a few colleagues and I decided to start truly academic Information Security Conference in Dallas and see what happens. We held the first DallasCon in 2002, just a few months after the tragic events of September 11, 2001 in the U.S. The response was overwhelming with academic papers being presented from as far away as Russia and attending coming from countries such as Japan and China.

**Astalavista** : There are so many active security cons and conferences out there that it is sometimes hard to decide which one is worth visiting. What, in your opinion, makes a con/conference qualified? Do you think that although there's nothing wrong with commercialization, some cons are becoming too commercial so they have lost sight of

what their vision used to be in the very beginning of their history?

**Bruce** : Truly, I must admit the lure of money being thrown at many of similar conferences such as ours is

sometimes overwhelming. When a company such as Microsoft comes knocking on your door with a fist full of cash

wanting to buy into a Keynote speaker slot, it's hard to resist the temptation to give in. But we have tried to separate

the academics from the commercial side. The training courses and the conference itself are designed to present the

latest unbiased view of current trends in information security. We have a team of dedicated colleagues that read

every paper carefully and look for flagrant promotions of certain technologies or companies. They also work very

closely with the speakers who are chosen to present at DallasCon, to make

sure that they know what is expected from them. We do offer sponsorship opportunities to companies to help us

carry the costs of such an event, but we try very hard to separate the business side from what people come to

DallasCon for, which is the latest unbiased view of the trends and research in information security. I think many

conferences lose sight of what made

them big and forget their roots.

**Astalavista** : Like pretty much every organization, ChoicePoint or T-Mobile, keep a great deal of personal, often sensitive information about us, as citizens, students or employees. What actions do you think should be taken by the general public, the companies themselves and the government to ensure that the security within such databases

125

or service providers is well beyond the acceptable level of security for most organizations?

**Bruce** : I think companies need to stop treating their customers like numbers and really put a face with the information that they are gathering. When someone gives you detailed information about themselves, they have put their trust in your company to protect them. When a breach is made, the customer feels betrayed and may never come back to you to do business. I laugh when I hear that huge multi-billion dollar companies are constantly having their customer data stolen. I wonder how much they are really spending on security? How much are their customers worth to them? These days it is hard to distinguish between legitimate companies and fake ones online. It's funny, but people have trouble revealing their credit card information or social security number to a physical business down

the street, but put the same business online and people throw that information at you without thinking twice. I

think consumers need to stop taking security for granted and use some common sense. The first step of security is common sense...You can't put a price on that!

**Astalavista** : Two words - Symbian and malware - what are your assumptions for the future trends on the mobile malware front?

**Bruce** : I predict that it will be huge. The future of mobile OS is wide open and as the competition for market

share grows, mobile companies want to offer anything they can in a smart-phone. I am always surprised as to what

phones can do right now... in a few years, they might even serve us breakfast in bed! The downside is the huge

vulnerability of the mobile-OS. First of all, more people own phones than computers around the world. It is the

obvious next frontier for virus writers. Secondly, theoretically, it is much easier to infect an entire phone network than PC's. All you need is one infected phone syncking with a base station. Again, I go back to my previous answer, people need to use common sense... Do you really need to put your financial data or your sensitive e-mail on your phone?

**Astalavista** : What is your opinion about the mass introduction of biometrics on a world wide scale?

**Bruce** : Good - it will make security more individualized. We will all carry our security inside our DNA. Bad - it might increase the market for organ theft! (just kidding!)

**Astalavista** : In conclusion, I would appreciate if you share your comments about the Astalavista.com site, and particularly about this security publication?

**Bruce** : I have been visiting Astalavista.com for many years now, and I am very

impressed with the up to date cutting edge news, articles and really underground topics covered on your site. When

we wanted to really reach out to the educated hacker community, Astalavista.com was the obvious choice. Thanks

for putting us on your site and thanks for helping us promote our event.

**Astalavista** : You're welcome, wish you luck with the con!

-----

**Interview with Nicolay Nedyalkov,**  
[13]<http://www.iseca.org/>

**Astalavista** : Hi Nicolay, would you, please, introduce yourself to our readers and share some info about your

experience in the information security industry? Also what is ISECA all about?

**Nicolay** : My interest in information security dates back from 1996. At that time, respected Bulgarian experts

from all over the country used to meet periodically at closed seminars where we exchanged our ideas and experi-

ence. At a later stage we developed the phreedom.org E-zine. I have also participated in numerous national and international mathematics and IT contests.

126

Currently I am a managing director for the R &D; department of one of Bulgaria's most Prominent IT companies – Information Service. In 2002 I decided to initiate an InfoSec course at the University of Sofia. Once the course

“Network Security? became part of the university's curriculum, we immediately got the interest of over 500 students.

During 2003, with the help of several experienced security colleagues of mine we developed another fresh and very useful course in “Secure programming?. Both of the courses fitted perfectly into the program curriculum and actually they attracted more students than we had expected. I am also teaching four other courses in Software technologies.

As a whole, we contributed for the development of IT education in Bulgaria establishing the ISECA (Information Security Association), whose main purpose is to connect our members and inspire them to innovate, create, and enrich their personal knowledge, while being part of a unique community.

**Astalavista** : Correct me if I'm wrong but I believe not many Eastern European universities emphasize on the practicality of their computer and network security courses? What are your future plans for enriching the course selection further, and also integrating a more practical approach into your curriculum ?

**Nicolay** : During the last couple of years we have seen a definite slowdown in Europe regarding information security courses and programmes. Until now we have already developed over eight courses, including the course Information Systems Security Audits, which is widely applicable. Further, there is intensive work on the development of a new Network & Software Security Lab. We are also negotiating with ABA representatives for the introduction of a professional certification program - "Risk Management in the Financial and Banking Sector?"

In fall 2005, University of Sofia will start a specialized master Information Security Program, coordinated by ISECA.

**Astalavista** : Who are the people behind ISECA, and what are the current local/global projects you're working on, or intend to develop in the upcoming future?

**Nicolay** : Our core members include certified security consultants and auditors, researchers, IS managers and



class teaching professors. Among the key projects we've already developed or we are working on at the moment are:

- A National Laboratory for Network and Software Audits, being developed in close cooperation

with The University of Sofia. The lab will be used for audits and R &D; in the industry.

- An Information Security Portal - ISECA

- A National anti-spam system and its integration within international ones like SpamHouse

- Safeguarding the local business interests of information security and promoting its development on a government level

- Active participation in the development of the Bulgarian Law for E-trade and E-signature

- Subscription based "Vulnerability Notification? service

- Centralized log analysis and security monitoring

**Astalavista** : What is the current situation of the Bulgarian IT and Security market? What was it like 5 years

ago, and is there an active security scene in the country?

**Nicolay** : We are currently witnessing a boom in the Bulgarian demand for information security services as a

great number of businesses are realizing the importance of information security. On the other hand we are in a

process of building strategical relationships with Bulgarian and multinational companies providing security related products and services. In the last couple of years official government bodies also have emphasized on sustaining secure communications. In response, our main goal in the upcoming future would be to build a collaborative working atmosphere with stable relationships between key partners and experts

**Astalavista** : Bulgaria and Eastern Europe have always been famous as a place where the

127

first computer viruses actually originated, to name the Dark Avenger as the most famous author. What do you think caused this - plain curiosity, outstanding programming skills, or you might have something else in mind?

**Nicolay**: It is a fact that Bulgaria is popular with its potential in the creation of viruses, trojans and malware at all. The thing is that there are a great number of highly skilled experts, who cannot apply their talent in the

still growing local market; consequently they sometimes switch to the dark side. One of our main aims is namely

to attract people with great potential and provide them with a professional and stable basis, on which they could

develop themselves on the right track. The Bulgarian – Dark Avenger, well, he used to be an idol for the virus writers

and the name still brings respect.

**Astalavista** : Is there an open-source scene in Bulgaria, how mature is it, and do you believe the country

would be among the many other actively adopting open-source solutions in the future, for various government or nation's purposes?

**Nicolay** : Yes, there is a [14]Free Software Society . Several municipalities have already

turned into E-municipalities with the help of open source software. There was a proposition for the introduction of a

law for integrating open source software within the government's administration, which was unfortunately rejected

later on. Free Software Society is in close contact with various political movements, which reflects the overall

support and understanding of open source from the society. The use of open source is also within the objectives

of one of the main political parties in the country, a goal that resulted from the many initiatives undertaken by the

Free Software Society. ISECA's members are also active participants in the core direction of the FSS. We are cur-

rently developing a new opensource research team, part of Information Service – OSRT (Open-Source Research Team).

**Astalavista** : How skilled is the Bulgarian IT labor market and do you think there's a shortage of well - trained

specialists in both IT and Information Security? How can this be tackled?

**Nicolay** : There are a great number of highly qualified software developers in Bulgaria, who created the [15]Bulgarian Association for Software Developers. We have had numerous seminars and lectures between ISECA and the Association. One of our main objectives is namely to locate and unite the highly qualified IT and Security experts within Bulgaria. Both organizations are constantly seeking to establish stable relations with international organizations with the idea to exchange experience and promote mutually beneficial partnerships.

**Astalavista** : India is among the well-known outsourcing countries for various IT skills, while on the other hand the Bulgarian programmers are well- respected all over the world, winning international math and programming contests. Do you think an intangible asset like this should be taken more seriously by the Bulgarian Government, and what do you think would be the future trends?

**Nicolay** : Every year there is a leakage of highly qualified young professionals with great potential for growth, looking for further career development . The core reason for this “brainwave?”, so painful for the Bulgarian economy and society, is the lack of a relevant government policy, ensuring stable and beneficial career opportunities for the young generation. I honestly hope that further government policies, not only those related to the IT industry, would

be successful in providing what a nation needs – a bright future for its brightest minds.

**Astalavista** : In conclusion, I wanted to ask you what is your opinion of the Astalavista.com's web site and, in particular, our security newsletter?

**Nicolay** : I have been visiting Astalavista.com since its early days and it is great to see that recently the portal has successfully established among the few serious and comprehensive sites. Furthermore, you can always find whatever you are looking for - software, as well as recommendations and shared experience in information security.

128

I believe Bulgaria needs the same high quality portal, one of our main ideas behind ISECA.

**Astalavista** : Thanks for your time!

-----

**Interview with Roman Polesek,**  
[16]<http://www.hakin9.org/>

**Astalavista** : Hi Roman, would you please introduce yourself, share some info about your background in the security industry, and tell us what is Hakin9 all about?

**Roman** : My name is Roman Polesek, I am an editor-in-chief of the '[17]hakin9 - practical protection' maga-

zine since Summer of 2004. I'm 27 years old if it does matter. This might be a bit surprising for folks who know our magazine well, but I'm more a journalist/editor (and that is my education) than a CS/security master. Of course, I worked as a sysadmin for some time,

use mainly Unices and code in several languages, but in the IT industry world I'm rather a self made man. I suppose I

have no right to call myself "[18]a hacker" in the proper meaning of the word. In short, 'hakin9' - subtitled as "Hard Core IT Security Magazine" - aims to be a perfect source of strictly technical, IT security related quality information.

We noticed that both the market and the community lack comprehensive, in-depth works on this topic. Decision

was pretty simple: "Let's do it and let's do it good - we cannot fail". At the moment, with total circulation of nearly 50 thousand copies, we have 7 language versions. The magazine is available worldwide, by subscription or

in distribution. However, it's important to remember that we are not encouraging anyone to commit any criminal

acts. Beside disclaimers published in every issue of the mag, we emphasize on the legal matters wherever possible.

We do not want to make a magazine for the so-called script-kiddies and assume that our readers are professionals

and require some portion of knowledge to fully utilize magazine's content. On the other hand, as we all know, "The information wants to be free".

There's no reason to avoid any particular subjects. Every article that precisely describes an attack technique includes

a section that is to help defending from the threat we present. 'hakin9' is not only a magazine. The free cover CD is

attached to every hardcopy. The disc includes a live Linux distribution called [19]'hakin9.live' along with plenty of

useful documentation [RFCs, FYIs, HOWTOs] and a really huge amount of computer/network security applications.

We also prepare our own tutorials that allow readers to exercise the techniques described in articles [only in their

very own networks!]. Since the next issue of 'hakin9', the CD will also contain full versions of commercial applications for Windows. Although we rarely use Microsoft Windows, we consider it useful and some of the readers requested

such software. One of the articles from each issue is available for free, just to make sure anyone that buys 'hakin9'

won't regret the purchase. See our website if you're interested in trying 'hakin9' articles.

**Astalavista** : What do you think are the critical success factors for a security oriented hard cover magazine?

**Roman** : I am convinced that the crucial matter is honesty. Our target readers are highly educated, extremely

intelligent people and would easily recognize any marketing lies. We just do not say things that aren't true. Everyone

can see what we publish and how we do it. The other important thing is diversity. It's obvious that creating a

magazine that fits everybody is impossible. There will always be a guy that is not satisfied with, say, the cover story

or the layout or anything else. This is nothing unusual, but should be expressed loud and

clear. That's why we cover different topics – from e.g. attacks on Bluetooth stack, through data recovery in Linux or

anti-cracking techniques for Windows programmers to methods of compromising EM emissions. Last but not least,

the mother of all successes is making

people aware of magazines' existence. Nobody would buy 'hakin9' unless they know we are available. But

the main thing is that magazines like ours will never be mass publications, they have their niche that needs to

be cultivated. The general rule – for all press publishers, not only us – is "Respect your readers and they will

respect you". Selling many copies of one issue, using lies and misleading information, is not difficult. What's diffi-129

cult is to make sure that users will consider you a professional who just makes a good magazine, not a travelling agent.

**Astalavista** : What is the current situation on Poland's IT and Security scene, and do you think it's developing



in the right direction from your point of view, beside Poland's obvious anti-software patents policy?

**Roman** : Yes, "Thank you Poland" and all. It's always nice to know that someone in the world has positive connotations with your country. But I cannot give you any general overview of the Polish scene. It's just too diverse

and I work with IT specialists from all over the world, so I do not concentrate on Poland particularly. After all, most of the important things happen in the USA. Really, the main problem in Poland is software piracy. I'm not talking about

P2P networks specifically, I'm talking about the consciousness of Polish people. They are just not aware of the

fact that using cracked apps is a crime, a pure theft. I suppose this problem is present in all countries. And poverty

does not justify such a procedure at all, we have plenty of free substitutes for even the most popular software. The

Polish scene (I mean community by that, of course) is not very different from any other country. We do have a very

strong group of open source ideologists (some might call them the followers of Richard Stallman :)), we do have

some anti-patent people (I'd recommend <http://7thguard.net> for those who understand Polish). But we do not have

any spectacular successes with any real inventions or discoveries (mind

that for now I'm talking about the community, not the corporations). I'd only mention two phenomena your readers

might have heard of. One is the LSD, [Last Stage of Delirium] an independent research group known for pointing

out bugs in Microsoft RPC some years ago. The other well known is [20]Michal "Icamtuf" Zalewski, an author of a powerful passive network scanner called "p0f" and a set of very useful debugging/binary analysis called "fenris". The reason for this unimpressive situation is the fact that Poland was cut off from the capitalist world for nearly 50 years

[and ENIAC was introduced in 1947], so we were isolated from real computing during that time. We just have to

make these 50 years in the next few years. On the other hand, IT specialists from Poland – say, programmers – are

considered very ingenious and good workers. For offshore corporations they are really attractive.

**Astalavista** : During 2004/2005 we've seen record breaking \*reported\* vulnerabilities. What do you think is

the primary reason, increasing Internet population, programmers' deepening their security knowledge, companies

in a hurry to integrate more features with a trade-off in security or perhaps something else?

**Roman** : All of them.

The increasing number of Internet users does not directly influence the number of

vulns found, though. The new Internauts are mainly people who have never used computers and networks before.

Of course the other thing is that Internet "aggregates" huge amounts of data, which was publicly unavailable before.

There are more and more programmers and IT security specialists. Their population is constantly growing, be it

because of the money they can earn or just the popularity of Computer Sciences. To be honest, most of them are at

most average at their job, but for example people from India and China have great potential.

But you are right. Marketing and pressure for higher sales make companies work in a great hurry, they just don't care

about average Joe Sixpack. And Joe Sixpack would hardly ever notice any security vulnerabilities, not mentioning

they would probably never report such flaws. Finding bugs in software has also become some kind of a fashion these

days. It's an intellectual challenge, similar to solving riddles. No wonder that along with the increasing number of

people able to understand, say, the C code, the number of vulns reported increases. There is one more thing I'd

like to mention. I suppose that the scale of reported vulns would appear far greater if proprietary software creators

informed about all flaws found in their products. It's not in their interest of course.

**Astlavista** : Thought or at least positioned to be secure, MAC's and Firefox browsers have started putting a

lot of efforts to patch the numerous vulnerabilities that keep on getting reported. Is it the design of the software

itself or the successful mass patching and early response procedures that matters most in these cases?

**Roman** : I have great respect for Apple products, though the only Mac I use is a very old Performa :), just for

experiments with BSD distributions. I consider Macs secure in general. I also use Mozilla Firefox daily. I'd bet on the

130

latter case, but like I said I'm no programming guru. The developers try to act fast and release patches as soon as possible, so at least average users can feel secure. The fact that there are plenty of developers makes it only better.

Bugs in the code are not a nemesis themselves, you cannot avoid bugs in more complex applications. The only

solution that makes sense for me is to conduct constant audits and release patches frequently. Look at the Microsoft

Internet Explorer [I am aware this example is a

bit trivial]. I have a feeling that this company's ways of dealing with flaws is just childish, reminds me of covering your own eyes and hoping it will make yourself invisible to other kids on the playground. I'm not criticizing Microsoft at all

- it's just that the company with so many great specialists has problems with securing their code, and their software

is the most popular solution in the world, no doubt. Apple is competing with Windows in general and Firefox tries to

bite a part of the browser market. Looking at their financial and market share results makes me sure that the way

the patches are done by these enterprises are the only right solution. Repeating that your product is secure and just

better does not make it secure and better.

**Astalavista** : In may, a DNS glitch at Google forwarded its traffic to [21]www.google.com.net (GoSearchGo.com) for 15 minutes. What are your comments about this event when it comes to security and mass DNS hijacking attempts

on a large scale? Do you also picture a P3P enabled Google used on a large scale in the near future and do you fear

that Google might be the next

data aggregator (they are to a certain extent) breached into?

**Roman** : The real point is – DJB mentioned that in an interview for the next issue of 'hakin9' – that some of

the protocols we use, especially SMTP and DNS, are outdated. To be precise, they were outdated at the moment they

were being created. It's nobody's fault. We have a saying in Poland that "Nobody is a prophet in his own country".

Even Bill Gates didn't notice the potential of the Internet. I would say Google has really nothing to do with any DNS

forgery. The protocol is flawed. What's worse, we can live without the problematic SMTP. Without DNS, which is a

core of the Internet. For example, I just cannot imagine my mother using IP addresses to surf the WWW. I'm not

afraid of threats to Google security. They have technology, they have money, they have ideas. I might say that it's

Google, which will start and force security improvements in domain resolving mechanism. Daniel J. Bernstein claims

that the first thing we should do is to implement some method of authentication in DNS protocol. Be it PKI, be it

anything else - we have to do it so that we would have some time to introduce a really secure DNS replacement. As

for the hijacking itself, I consider it one of the most primitive kinds of abusing IT infrastructure. It's just like taking over somebody's house. It's as bad as deleting someone's data for sports or DDoS attacks used for fun and/or profit.

**Astalavista** : Anonymous P2P networks have been getting a lot of popularity recently namely because of RIAA's

lawsuits on a mass scale. How thin do you think is the line between using P2P networks to circumvent censorship in

Orwellian parts of the world, and the distribution of copyrighted materials?

**Roman** : 'hakin9' team likes P2P networks, the more anonymous, the better. We use them for distributing

our free articles and our CD. It makes me laugh when \*\*AAs send e-mails with legal threats based on the American

legal system to Polish or Swedish citizens. Sometimes they're like an old blind man in the fog. Instead of adopting P2P

for selling their video or music, they make the community angry. Digressions aside. I don't feel that P2P networks will

help anyone make their transfers safe [security through obscurity, right?] and that they will help to fight censorship

in countries like North Korea or even China. On the other side, I can imagine modifying XMPP [Jabber] protocol to

transfer SSL-secured data – it may be already done, I had no time to investigate it further. Unauthorized distribution

of copyrighted content, however, will always be a problem. There's no way to prevent such behaviour. Recent events

show us that writing a P2P client is a piece of cake, even a clever 9 years old boy can do this. I would rather make it

easier for people to buy electronic copyrighted materials without the need to download it illegally. Regarding that

according to some statistics even 30 per cent of total internet transfers are generated by P2P networks, I'm rather

afraid that some stupid people downloading pr0n or Britney Spears MP3s could easily kill the Net some day. To sum

up, each technology has its profits and costs. Obvious :). The profit of P2P is the ease of distributing any content. The cost is the people using it in an illegal manner. I can see no reason for prohibiting these network just because some

people prefer bad quality motion pictures to going to the movies. Should we prohibit usage of knives only because of the fact that someone stabbed the kitchen knife in someone's stomach?

**Astalavista** : In conclusion, I wanted to ask you what is your opinion of the Astalavista.com's web site, in particular, our security newsletter?

**Roman** : I'm very impressed with the amount of data available for Astalavista's visitors. I'm not a member though, so I cannot really make a detailed review. To be honest, I had some problems with recognizing which of your websites are free and which ones are not. But I have managed to do it and use it almost daily :). As for the newsletter, it's one of the most informative and professional ones I have ever seen. Since having read Issue 16, I couldn't stop myself from reading the archives. I am a subscriber and strongly advise everybody to do the same. As a person professionally dealing with IT security, I mean it - this is not an advertisement for Astalavista. This is the truth.

**Astalavista** : Thanks for your time Roman!

-----

**Interview with John Young,**  
[22]<http://www.cryptome.org/>

**Astalavista** : Hi John, would you, please, introduce yourself to our readers, share some info on your back-



ground, and tell us something more about what are Cryptome.org and the Eyeball-Series.org all about?

**John** : Cryptome was set up in June 1996, an outgrowth of the Cypherpunks mail list. Its original purpose

was to publish hard to get documents on encryption and then gradually expanded to include documents on

information security, intelligence, national security, privacy and freedom of expression. Its stated purpose now

is: "Cryptome welcomes documents for publication that are prohibited by governments worldwide, in particular

material on freedom of expression, privacy, cryptology, dual-use technologies, national security, intelligence, and

secret governance – open, secret and classified documents – but not limited to those. Documents are removed

from this site only by order served directly by a US court having jurisdiction. No court order has ever been served;

any order served will be published here – or elsewhere if gagged by order. Bluffs will be published if comical but

otherwise ignored." The Eyeball Series was initiated in 2002 in response to the US government's removal of public

documents and increased classification. Its intent is to show what can be obtained despite this clampdown.

**Astalavista** : What is your opinion about cyberterrorism in terms of platform for education, recruiting, propa-

ganda and eventual real economic or life losses?

**John** : Cyberterrorism is a threat manufactured by government and business in a futile attempt to continue

control of information and deny it to the public. Cyber media threatens authorities and authoritarians so it is

demonized as if an enemy of the state, and, not least,

corporate profits.

**Astalavista** : A couple of words - privacy, data aggregation, data mining, terrorism fears and our constantly

digitized lives?

**John** : Privacy should be a right of citizens worldwide, in particular the right to keep government and business

from gaining access to private information and personal data. The argument that government needs to violate

privacy in order to assure security is a lie. The business of gathering private information by corporations and then

selling that to government and other businesses is a great threat to civil liberties. Much of this technology was

developed for intelligence and military uses but has since been expanded to include civil society.

**Astalavista** : Shouldn't the U.S be actively working on hydrogen power or alternative power sources instead

132

of increasing its presence in the Middle East or to put the question in another way, what is the U.S doing in Iraq in

your opinion? What do you think is the overall attitude of the average American towards these ambitions?

**John** : No question there should be energy sources as alternatives to the hegemonic fossil fuels. Dependence

on fossil fuels is a rigged addiction of that worldwide cartel. Car ads are the most evil form of advertising, right up

there with crippling disease of national security.

**Astalavista** : Is ECHELON still functioning in your opinion and what do you believe is the current state of global communications interception? Who's who and what are the actual capabilities?

**John** : Echelon continues to operate, and has gotten a giant boost since 9/11. The original 5 national benefi-

ciaries – US, UK, CA, AU and NZ – have been supplemented by partial participation of other nations through global

treaties to share information allegedly about terrorism. Terrorism is a bloated threat, manufactured to justify huge

funding increases in

defense, law enforcement and intelligence budget around the globe. Businesses which supply these agencies have

thrived enormously, and some that were withering with the end of the Cold War have resurged in unprecedented

profits, exceeding those of the Cold War.

**Astalavista** : Network-centric warfare and electronic warfare are already an active doctrine for the U.S govern-

ment. How do you picture the upcoming future, both at land and space and might the Wargames scenario become reality some day?

**John** : Network wargames are as pointless and wasteful as Cold War wargames were. They churn activity and consume expensive resources. None are reality-based, that is, outside the reality of imaginary warfare.

**Astalavista** : Do you believe there's currently too much classified or declassified information, namely documents, maps, satellite imagery etc. available on the Net these days? In the post 9/11 world, this digital transparency is obviously very handy for both terrorists and governments, but who do you think is benefiting from it?

**John** : Far from being too much information available to the public, there is a diminishing amount, especially about exploitation of those who have access to classified and "privileged" information – government and business – and those who lack access. The concocted warning that open information aids terrorism is a canard of great legacy, one that is customarily spread during times of crisis, the very times when secret government expands and becomes less accountable. "National security" is the brand name of this cheat.

**Astalavista** : In conclusion, I wanted to ask you what is your opinion of the Astalavista.com's web site, in par-

ticular, our security newsletter?

**John** : Great site, very informative, give yourself a prize and a vacation at G8 with the world class bandits.

**Astalavista** : Thanks for your time John!

**John** : Thanks to you!

-----

1. <http://www.snake-basket.de/>

2. <http://www.warindustries.com/>

3. <http://www.dallascon.com/>

4. <http://www.iseca.org/>

5. <http://www.hakin9.org/en/>

133

6. <http://www.cryptome.org/>

7. <http://ddanchev.blogspot.com/2006/01/security-interviews-20042005-part-1.html>

8. <http://ddanchev.blogspot.com/2006/01/security-interviews-20042005-part-3.html>

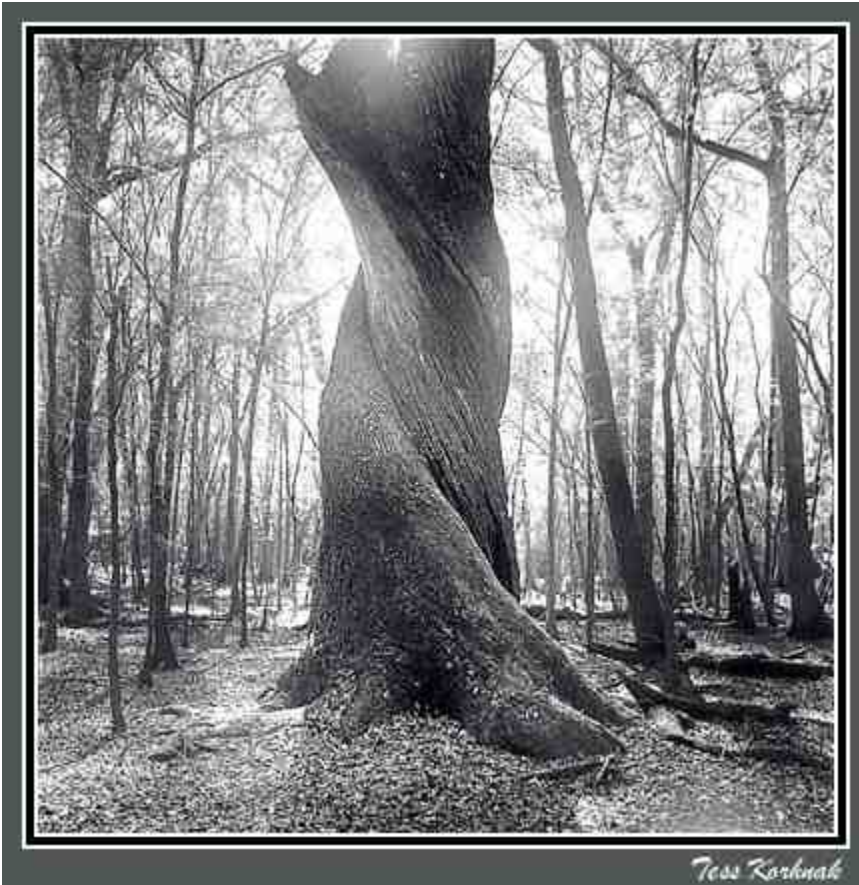
9. <http://www.astalavista.com/index.php?section=newsletter>

10. <http://www.snake-basket.de/>

11. <http://www.warindustries.com/>

12. <http://www.dallascon.com/>

13. <http://www.iseca.org/>
14. <http://www.fsa-bg.org/>
15. <http://devbg.org/en/>
16. <http://www.hakin9.org/>
17. <http://hakin9.org/en>
18. <http://www.catb.org/~esr/jargon/html/H/hacker.html>
19. [http://www.haking.pl/en/index.php?page=hakin9\\_live](http://www.haking.pl/en/index.php?page=hakin9_live)
20. <http://lcamtuf.coredump.cx/>
21. <http://www.google.com.net/>
22. <http://www.cryptome.org/>



Google 视着我们的搜索结果的业务作为一种优质服务。我们提供快速和公正搜索结果给我们的用户。我们停止站点的与非法页只在负责任是对那些真的网站站长请求下，当这是spanning 我们的索引，或提法律要求。这项政策是必需保证页从我们的索引不是当地不被删除。

## Twisted Reality (2006-01-30 18:15)

[1]

I looked up the [2]definition of Evil today, and I found it, I tried to play a Google War and came across 256 million

[3]occurrences of it, still there's a [4]hope for all of us I guess. On the 17th of January I blogged on how [5]China

turned into the biggest black spot on the Internet's map, to find out that I even have activists commenting in my blog

:)

Google has agreed to "[6]remove certain sensitive information from our search results" you all know it by now, what you perhaps don't know is how what used to be the old Google still has its marks on the web. [7]Google's

Information for Webmasters still states that :

*"Google views the comprehensiveness of our search results as an extremely important priority. We're committed to providing thorough and unbiased search results for our users."*

[8]

I guess Chinese users should print this and stick it on their walls to remind them of the past as it says exactly the

same. They have also [9]removed their "censored notice" from "older removals", how come, and for what reason?

Lack of accountability for when "local laws, regulations, or policies" were removing "sensitive information" before the date?! Google is my benchmark for disruption, but I guess its actions and "do no evil" motto were simply too pure for the business world, which on the majority of occasions is capable of destroying morale, even individuals..

Welcome in a [10]"Twisted Reality" where one event looks like an entirely different one - on request, and the list is getting [11]bigger!





[12]

But what is actually filtered in china these days, what are the topics of interest? Four years ago, a [13]great initiative brought more insights into what's deemed "sensitive information", and while of course the list is changed on-the-fly, it is important to know how it blocks the top results, as this is where all the traffic goes.

Recently, CNET did a nice [14]research on which sites are blocked by which search engine, I ever saw [15]Neworder

in there :)

[16]

136



The best thing about [17]China's backbone is how centralized it really is and the way [18]researchers are finding

[19]common censorship patters that could prove useful for future research. Is [20]TOR with its [21]potential

applicable in China, and would initiatives such as the the [22]Anonymous OS, or even [23]TorPark, an USB extension

of the idea, the future?

Meanwhile, in case they are interested parties reading this post, consider taking a look at the "[24]Handbook for

Bloggers and Cyber-Dissidents" courtesy of [25]Reporters Without Borders.

Technorati tags :

[26]privacy, [27]censorship, [28]search engine, [29]google, [30]china, [31]TOR, [32]Anonymity

1. <https://web.archive.org/web/20101016193525/http://www.sfrc.ufl.edu/Larry/twisted.jpg>
2. <http://www.google.com/search?hl=en&q=define%3Aevil>
3. <http://www.google.com/search?hl=en&q=evil>
4. <http://www.google.com/search?hl=en&lr=&q=good>
5. <http://ddanchev.blogspot.com/2006/01/china-biggest-black-spot-on-internets.html>
6. <http://googleblog.blogspot.com/2006/01/google-in-china.html>
7. <http://www.google.com/webmasters/remove.html>
8. [https://web.archive.org/web/20101016193525/http://photos1.blogger.com/blogger/1933/1779/1600/google\\_china.1.jpg](https://web.archive.org/web/20101016193525/http://photos1.blogger.com/blogger/1933/1779/1600/google_china.1.jpg)
9. <http://www.google.com/support/bin/answer.py?answer=17795&topic=368>
10. <http://www.google.cn/>

11. <http://blog.outer-court.com/censored/>
12. <https://web.archive.org/web/20101016193525/http://blog.outer-court.com/files/google-images-censorship.jpg>
13. <http://cyber.law.harvard.edu/filtering/china/google-kw-chart.html>
14. [http://news.com.com/What+Google+censors+in+China/2100-1030\\_3-6031727.html](http://news.com.com/What+Google+censors+in+China/2100-1030_3-6031727.html)
15. <http://neworder.box.sk/>
16. <https://web.archive.org/web/20101016193525/http://blog.outer-court.com/files/google-images-censorship-china.jpg>
- 137
17. <http://www.cnnic.net.cn/images/2004/image/map2003q4.jpg>
18. <http://ice.citizenlab.org/>
19. <http://ice.citizenlab.org/documents/ProjectC-r1.pdf>
20. <http://tor.eff.org/>
21. <http://www.noreply.org/tor-running-routers/>
22. <http://theory.kaos.to/projects.html>
23. <http://www.freehaven.net/~arrakis/torpark.html>

24.

[http://www.rsf.org/IMG/pdf/handbook\\_bloggers\\_cyberdissidents-GB.pdf?PHPSESSID=5f53e6cb837bd734cc0c945eaf7](http://www.rsf.org/IMG/pdf/handbook_bloggers_cyberdissidents-GB.pdf?PHPSESSID=5f53e6cb837bd734cc0c945eaf7)

[512a1](#)

25.

<https://web.archive.org/web/20101016193525/http://www.rsf.org/>

26. <http://technorati.com/tag/privacy>.

27. <http://technorati.com/tag/censorship>

28. <http://technorati.com/tag/search+engine>

29. <http://technorati.com/tag/google>

30. <http://technorati.com/tag/china>

31. <http://technorati.com/tag/TOR>

32. <http://technorati.com/tag/Anonymity>

138



**How we all get Own3d by Nature at the bottom line?  
(2006-01-30 18:17)**

[1]

I just came across a clip courtesy of [2]NASA that can be described as a [3]beau-

tiful devastation, still it reminds me of how insecure we are at the bottom line. And no, I don't see how you will

distribute a signature for this, or can you? :)

Technorati tags :

[4]katrina, [5]security

1. [https://web.archive.org/web/20101016193525/http://photos1.blogger.com/blogger/1933/1779/1600/katrina\\_hurricane\\_2005.jpg](https://web.archive.org/web/20101016193525/http://photos1.blogger.com/blogger/1933/1779/1600/katrina_hurricane_2005.jpg)

2. <http://www.nasa.gov/>

3. [http://www.nasa.gov/mov/133273main\\_katrina\\_GOES.mov](http://www.nasa.gov/mov/133273main_katrina_GOES.mov)

4. <http://technorati.com/tag/katrina>

5. <http://technorati.com/tag/security>

139



**Was the WMF vulnerability purchased for \$4000?!**  
**(2006-01-30 18:18)**

[1]

Going through Kaspersky's latest summary of [2]Malware - Evolution, October

- December 2005, I came across a research finding that would definitely go under the news radar, as always, and

while [3]The Hackers seem to be more elite than the folks that actually found the vulnerability I think the issue itself deserves more attention related to the future development of a [4]market for 0day vulnerabilities.

Concerning the [5]WMF vulnerability, it states :

*"It seems most likely that the vulnerability was detected by an unnamed person around 1st December 2005, give or take a few days. It took a few days for the exploit enabling random code to be executed on the victim machine to be*

*developed. Around the middle of December, this exploit could be bought from a number of specialized sites. It seems*

*that two or three competing hacker groups from Russian were selling this exploit for \$4,000. Interestingly, the*

*groups don't seem to have understood the exact nature of the vulnerability. One of the purchasers of the exploit is*

*involved in the criminal adware/ spyware business, and it seems likely that this was how the exploit became public."*

Two months ago, I had a [6]chat with [7]David Endler, director of Security Research at [8]TippingPoint, and their

[9]ZeroDayInitiative, that is an alternative to [10]iDefense's efforts to provide money as a incentive for quality

vulnerabilities submissions. The fact that a week or so later, the [11]first vulnerability appeared on Ebay felt "good"

mainly because what I was [12]long envisioning actually happened - motivated by the already offered financial

rewards, a researcher decided to get higher publicity, thus better bids. I never stopped thinking on who gains, or who

should actually gain, the vendor, the end user, the Internet as a whole, or I'm just being a moralist in here as always?

This very whole concept seemed flawed from the very beginning to me, and while you wish you could permanently

employ every great researcher you ever came across to, on demand HR and where necessary seems to work just

fine. But starting with money as an incentive is a moral game where "better propositions" under different situations could also be taken into consideration. Researchers will always have what to report, and once ego, reputation and

publicity are by default, it comes to the bottom line - the hard cash, not "who'll pay more for my research?", but

"who values my research most of everyone else?". And when it comes to money, I feel it's quite common sense to conclude that the underground, have plenty of it. I am not saying that a respected researcher will sell his/[13]her

research to a illegal party, but the a company's most serious competitors are not its current, but the emerging ones,

I feel quite a lot of not so publicly known folks have a lot to contribute..

**Possible scenarios on future vulnerability purchasing trends might be :**



- what if vendors start offering rewards ( \$ at the bottom line) for responsibly reported vulnerabilities to eliminate

the need of intermediaries at all, and are the current intermediaries doing an important role of centralizing such

purchases? I think the Full Disclosure movement, both conscious or subconscious :) is rather active, and would

continue to be. Now, what if Microsoft breaks the rules and opens up its deep pocketed coat?

- how is the 0day status of a purchased vulnerability measured today? My point is, what if the WMF vulnerability

was used to "nail down" targeted corporate customers, or even the British government as it actually [14]happened , and this went totally unnoticed due to the lack of mass outbreaks, but the author sort of cashed twice, by selling the

though to be 0day to iDefense, or ZeroDay's Initiative? What if?

140

- requested vulnerabilities are the worst case scenario I could think of at the moment. Why bother and always get excited about an IE vulnerability, when you know person/company X are running Y AV scanner, use X1 browser as a

security through obscurity measure. That's sort of reverse model compared to current one where researchers

"push" their findings, what if it turns into a "pull" approach, "I am interested in purchasing vulnerabilities affecting that version of that software", would this become common, and how realistic is it at the bottom line?

Some buddies often ask me, why do I always brainstorm on the worst case scenario? I don't actually, but try to

brainstorm on the key factors and how the current situation would inevitably influence the future. And while I'm not

Forrester Research, I don't charge hefty sums for 10 pages report on the [15]threats posed by two-factor

authentication or e-banking, do I? Still, I'm right on quite some occasions..

At the bottom line, ensure \$ isn't the only incentive a researcher is getting, and don't treat them like they are all the same, because they aren't, instead sense what matters mostly to the individual and go beyond the financial

incentive, or you'll lose in the long term.

What are you thoughts on purchasing vulnerabilities as far as the long term is concerned? What is the most effective

compared to the current approaches way of dealing with 0day vulnerabilities? Might a researcher sell his findings to

the underground given he knows where to do it? What do you think?

**UPDATE :** "[16]Where's my 0day, please?"

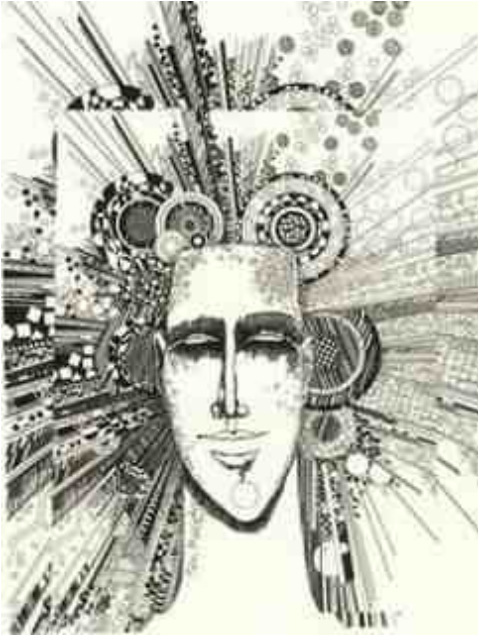
Technorati tags :

[17]security, [18]information security, [19]vulnerabilities, [20]underground, [21]0day vulnerability market, [22]WMF,

[23]Kaspersky, [24]malware

1. [https://web.archive.org/web/20101016193525/http://photos1.blogger.com/blogger/1933/1779/1600/hackers\\_6.2.jpg](https://web.archive.org/web/20101016193525/http://photos1.blogger.com/blogger/1933/1779/1600/hackers_6.2.jpg)
2. <http://www.viruslist.com/en/analysis?pubid=178619907>
3. <http://www.mgm.com/hackers>
4. <http://ddanchev.blogspot.com/2005/12/0bay-how-realistic-is-market-for.html>
5. <http://www.microsoft.com/technet/security/advisory/912840.mspx>
6. [http://www.astalavista.com/media/archive1/newsletter/issue\\_23\\_2005.pdf](http://www.astalavista.com/media/archive1/newsletter/issue_23_2005.pdf)
7. [http://www.voipsa.org/About/board\\_Endler.php](http://www.voipsa.org/About/board_Endler.php)
8. <http://www.tippingpoint.com/>
9. <http://www.zerodayinitiative.com/>
10. <http://www.idefense.com/>
11. <http://ddanchev.blogspot.com/2005/12/0bay-how-realistic-is-market-for.html>
12. <http://www.google.com/search?hl=en&lr=&q=0day+vulnerabilities+market&btnG=Search>
13. <http://www.invisiblethings.org/aboutme.html>
14. [http://news.zdnet.com/2100-1009\\_22-6029691.html](http://news.zdnet.com/2100-1009_22-6029691.html)

15. [http://www.trojan.ch/paper/ThreatsToOnlineBanking\\_Candid\\_Wueest.pdf](http://www.trojan.ch/paper/ThreatsToOnlineBanking_Candid_Wueest.pdf)
16. <http://ddanchev.blogspot.com/2006/03/wheres-my-0day-please.html>
17. <http://technorati.com/tag/security>
18. <http://technorati.com/tag/information+security>
19. <http://technorati.com/tag/vulnerabilities>
20. <http://technorati.com/tag/underground>
21. <http://technorati.com/tag/0day+vulnerability+market>
22. <http://technorati.com/tag/WMF>
23. <http://technorati.com/tag/Kaspersky>
24. <http://technorati.com/tag/malware>



## **January's Security Streams (2006-01-31 18:19)**

[1]

It's been quite a busy month, still I've managed to keep my blog up to date

with over 30 posts during January, here they are with short summaries. Thanks for the comments folks!

I often get the question, how many people is my blog attracting, the answer is quantity doesn't matter, but the

quality of the visits, still, for January there were 7,562 unique visits and over 13,000 pageloads. I'm already counting over 400 .mil sub domains, have the majority of security/AV vendors(hi!) reading it, and the best is how long they

spend on average, and how often they come back. To sum up, 60 % of all visits come from direct bookmark of my

blog, 30 % through referers, and 10 % from search engines. It is also worth mentioning my [2]last referring link,

notice the domain and what they are interested in.

- 1.** [3]What's the potential of the IM security market? Symantec thinks big" gives a brief overview of the wise acquisition Symantec did and a little something the IM security market.
- 2.** "[4]Keep your friends close, your intelligence buddies closer!" mentioning the release of a book excerpt and provides further resources on various NSA and intelligence related topics
- 3.** "[5]Security quotes : a FSB (successor to the KGB) analyst on Google Earth" is Google Earth or satellite imagery a national security threat? At least the Russian FSB thinks so!
- 4.** "[6]How to secure the Internet" discusses the U.S National Strategy to Secure Cyberspace and some thoughts on the topic
- 5.** "[7]Malware - Future Trends" the original announcement for the release of my research
- 6.** "[8]Watch out your Wallets!" gives more info on ID theft and talks about a case that left a 22 years old student in debt of \$412,000
- 7.** "[9]Would we ever witness the end of plain text communications?" a released report on the growth of VPNs prompted me to open up the topic, recently, Yahoo! communicate over SSL by default which is a great progress from  
  
my point of view
- 8.** "[10]Why we cannot measure the real cost of cybercrime?" an in-depth summary of my thoughts on why we 142

cannot measure the real cost of cybercrime, and why I doubt the costs outpace those due to drug smuggling **9.** "[11]The never-ending "cookie debate" tries to emphasize on how the Cookie Monster should worry about cookies only, and what else to keep in mind concerning further techniques that somehow invade your privacy

**10.** "[12]The hidden internet economy" here I argue on what would the total E-commerce revenues be given those afraid to purchase over the Internet actually start doing it.

**11.** "[13]Security threats to consider when doing E-Banking" provides a link to practical research conducted by a

[14]dude I happen to know :)

**12.** "[15]Insecure Irony" is indeed an ironical event, namely how a private enterprise, one used to gather intelligence actually lost sensitive info belonging to the [16]Intelligence Community

**13.** "[17]Future Trends of Malware" the post mentioning my Slashdotted research and the rest of the people and respected sites that recognized it

**14.** "[18]To report, or not to report?" how can you measure costs when the majority of companies aren't even reporting the breaches, cannot define a breach, or think certain breaches don't require law enforcement

intervention?

**15.** "[19]Anonymity or Privacy on the Internet?" argues on what exactly different individuals are trying to achieve, is it Anonymity, is it Privacy and provides further resources on the topic

**16.** "[20]What are botnet herds up to?" gives a brief overview of recent botnet herds' activities the ways used to increase the revenues through affiliate networks, or domaining. It also provides good resources on the topic of Bots

and Botnets

**17.** "[21]China - the biggest black spot on the Internet's map" a very recent and resourceful overview of Internet Censorship in China, that also provides further resources on the topic

**18.** "[22]FBI's 2005 Computer Crime Survey - what's to consider?" one day after the release of the FBI's survey I summarized the key points to keep in mind

**19.** "[23]Why relying on virus signatures simply doesn't work anymore?" a very practical post that argues and tries to build more awareness on how the number of signatures detected by a vendor doesn't actually matter, still there

are other solutions that will get more attention with the time. I received a lot of feedback on this, both vendors and

from folks I met through my blog, thanks for the ideas!!

**20.** "[24]2006 = 1984?" gives more details on private sector companies innovating in the wrong field, and further resources on censorship and surveillance practices

**21.** "[25]Cyberterrorism - recent developments" an extended overview of [26]Cyberterrorism, and a lot of facts worth mentioning obtained through a recently released report on the topic



**22.** "[27]Still worry about your search history and BigBrother?" Some humor, be it even a black one is always useful **23.** "[28]Homebrew Hacking, bring your Nintendo DS!" Homebrew hacking is slowly emerging and I see a lot of potential in the "do it yourself culture"

143

**24.** "[29]Visualization, Intelligence and the Starlight project" a post worth checkin' out, it provides an overview of various visualization technologies and talks about the Starlight project

**25.** "[30]The Feds, Google, MSN's reaction, and how you got "bigbrothered"?" I'm not coining new terms here,

"bigbrothered" is slowly starting to be used by pretty much everyone, yet I try to give practical tips on why the whole idea was wrong from the very beginning, and how other distribution vectors should also be considered

**26.** "[31]Personal Data Security Breaches - 2000/2005" I came across a great report summarizing the issue, and tried to highlight the cases worth mentioning, some are funny, others are unacceptable

**27.** "[32]Skype to control botnets?!" good someone is brainstorming, but that's rather unpractical compared to common sense approaches botnet herders currently use

**28.** "[33]Security Interviews 2004/2005 - Part 1" Grab a beer and start going through this great contribution, soon to appear at Astalavista itself!

**29.** "[34]Security Interviews 2004/2005 - Part 2" Part 2

**30.** "[35]Security Interviews 2004/2005 - Part 3" and Part 3

**31.** "[36]Twisted Reality" Everything is not always as it seems, and it's Google I have in mind :(

**32.** "[37]How we all get 0wn3d by Nature at the bottom line?" :)

**33.** "[38]Was the WMF vulnerability purchased/sold for \$4000?!" among the few vendors I actually trust released a nice summary no one seems to be taking into consideration, still I find it truly realistic given the potential of the

## [39]0day market for software vulnerabilities

Till next month, and thanks to all readers for taking their time to go through my research and contributions!

## Technorati tags :

[40]security, [41]information security

1.

<https://web.archive.org/web/20101016193525/http://photos1.blogger.com/blogger/1933/1779/1600/Mind%20blowin>

[g\\_Nicholas%20Cann.jpg](#)

2. <http://www.google.ru/search?>

[g=0day%20exploit%20price&hl=ru&amp;amp;amp;am  
p;amp;amp;amp;amp;amp;lr=&](#)

newwindow=1&start=10&sa=N

3. <http://ddanchev.blogspot.com/2006/01/whats-potential-of-im-security-market.html>

4. <http://ddanchev.blogspot.com/2006/01/keep-your-friends-close-your.html>

5. <http://ddanchev.blogspot.com/2006/01/security-quotes-fsb-successor-to-kgb.html>
6. <http://ddanchev.blogspot.com/2006/01/how-to-secure-internet.html>
7. <http://ddanchev.blogspot.com/2006/01/malware-future-trends.html>
8. <http://ddanchev.blogspot.com/2006/01/watch-out-your-wallets.html>
9. <http://ddanchev.blogspot.com/2006/01/would-we-ever-witness-end-of-plain.html>
10. <http://ddanchev.blogspot.com/2006/01/why-we-cannot-measure-real-cost-of.html>
11. <http://ddanchev.blogspot.com/2006/01/never-ending-cookie-debate.html>
12. <http://ddanchev.blogspot.com/2006/01/hidden-internet-economy.html>
13. <http://ddanchev.blogspot.com/2006/01/security-threats-to-consider-when.html>
14. <http://www.trojan.ch/>
15. <http://ddanchev.blogspot.com/2006/01/insecure-irony.html>
- 144
16. <http://www.intelligence.gov/>
17. [http://ddanchev.blogspot.com/2006/01/future-trends-of-malware\\_16.html](http://ddanchev.blogspot.com/2006/01/future-trends-of-malware_16.html)

18. <http://ddanchev.blogspot.com/2006/01/to-report-or-not-to-report.html>
19. <http://ddanchev.blogspot.com/2006/01/anonymity-or-privacy-on-internet.html>
20. <http://ddanchev.blogspot.com/2006/01/what-are-botnet-herds-up-to.html>
21. <http://ddanchev.blogspot.com/2006/01/china-biggest-black-spot-on-internets.html>
22. <http://ddanchev.blogspot.com/2006/01/fbis-2005-computer-crime-survey-whats.html>
23. <http://ddanchev.blogspot.com/2006/01/why-relying-on-virus-signatures-simply.html>
24. <http://ddanchev.blogspot.com/2006/01/2006-1984.html>
25. <http://ddanchev.blogspot.com/2006/01/cyberterrorism-recent-developments.html>
26. <http://ddanchev.blogspot.com/2005/12/cyberterrorism-dont-stereotype-and-its.html>
27. <http://ddanchev.blogspot.com/2006/01/still-worry-about-your-search-history.html>
28. <http://ddanchev.blogspot.com/2006/01/homebrew-hacking-bring-your-nintendo.html>
29. <http://ddanchev.blogspot.com/2006/01/visualization-intelligence-and.html>
30. <http://ddanchev.blogspot.com/2006/01/feds-google-msns-reaction-and-how-you.html>

31. <http://ddanchev.blogspot.com/2006/01/personal-data-security-breaches.html>
32. <http://ddanchev.blogspot.com/2006/01/skype-to-control-botnets.html>
33. <http://ddanchev.blogspot.com/2006/01/security-interviews-20042005-part-1.html>
34. <http://ddanchev.blogspot.com/2006/01/security-interviews-20042005-part-2.html>
35. <http://ddanchev.blogspot.com/2006/01/security-interviews-20042005-part-3.html>
36. <http://ddanchev.blogspot.com/2006/01/twisted-reality.html>
37. <http://ddanchev.blogspot.com/2006/01/how-we-all-get-Own3d-by-nature-at.html>
38. <http://ddanchev.blogspot.com/2006/01/was-wmf-vulnerability-purchased-for.html>
39. <http://ddanchev.blogspot.com/2005/12/0bay-how-realistic-is-market-for.html>
40. <http://technorati.com/tag/security>
41. <http://technorati.com/tag/information+security>

145

## **2.2**

### **February**

146

## **Suri Pluma - a satellite image processing tool and visualizer (2006-02-02 15:28)**

I just came across a great [1]satellite image processing software and decided to share it with my blog readers. Perhaps

that's a good moment to spread the word about my [2]RSS compatible feed, so consider syndicating it. To sum up :

*"Suri Pluma is a satellite image processing tool and visualizer. It can open the most common image formats*

*without importing to an internal format and minimizing the memory required for visualization. It is designed to be*

*modular and extensible. It has a measurement tool (distance and areas with error estimation) and geographical and*

*map coordinate information."*

Check out the [3]screenshots and consider [4]downloading it in case you're interested. Meanwhile, you can

also go through a previous post that's again related to [5]visualization.

Technorati tags :

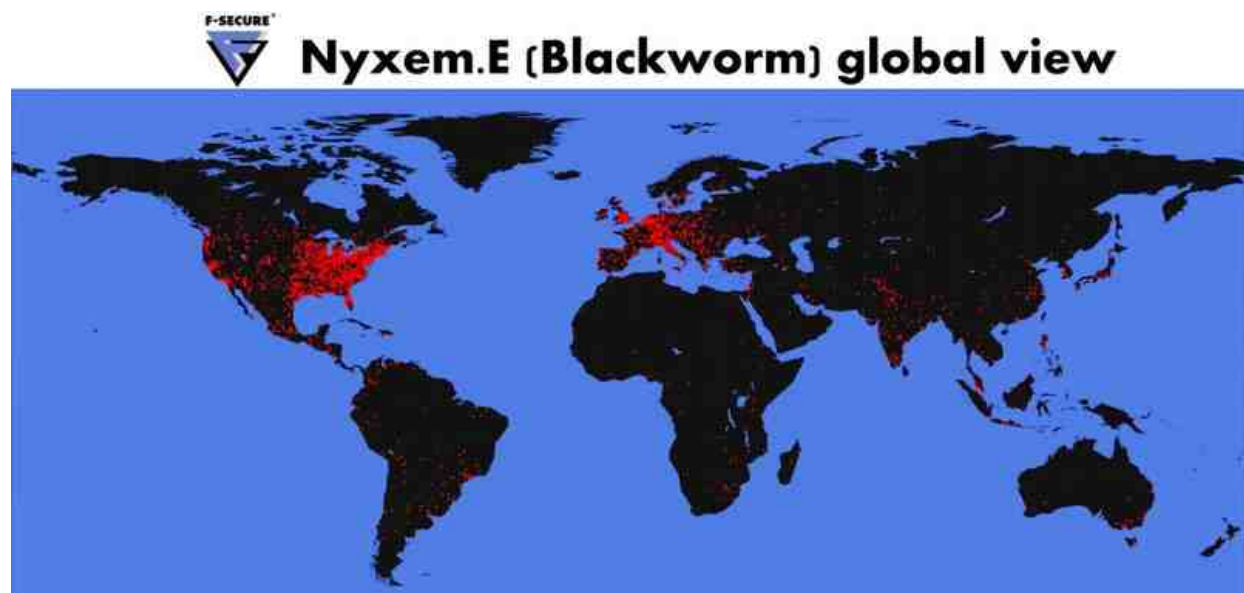
[6]satellites, [7]visualization, [8]Suri Pluma

1. <http://www.suremptec.com/suripluma.shtml>

2. <http://feeds.feedburner.com/DanchoDanchevOnSecurityAndNewMedia>

3. [http://www.suremptec.com/screenshots\\_en.shtml](http://www.suremptec.com/screenshots_en.shtml)
4. [http://www.suremptec.com/downloads\\_en.shtml](http://www.suremptec.com/downloads_en.shtml)
5. <http://ddanchev.blogspot.com/2006/01/visualization-intelligence-and.html>
6. <http://technorati.com/tag/satellites>
7. <http://technorati.com/tag/visualization>
8. <http://technorati.com/tag/Suri+Pluma>

147



**CME - 24 aka Nyxem, and who's infected? (2006-02-02 15:32)**

[1]

Today, the [2]F-Secure's team released a neat world map with the Nyxem.E infections. As you can see the U.S and

Europe have been most successfully targeted, but I wonder would it be the same given the author started [3]localizing the subject/body [4]messages found within the worm to other languages? Who seeks to cause damage instead of controlling information and network assets these days? A pissed off commodities trader? :) or on request, as the [5]original version of the worm "can perform a Denial of Service (DoS) attack on the New York Mercantile Exchange website (www.nymex.com)", still that's 2 years ago.

Tomorrow is the day when the worm should originally start deleting all all \*.doc, \*.xls, \*.mdb, \*.mde, \*.ppt,

\*.pps, \*.zip, \*.rar, \*.pdf, \*.psd and \*.dmp on an infected PC's, [6]supposedly network drives as well, what I also

expect is more devastation on the 3rd of March given the same happens every month. And while I doubt there's still

someone out there unaware of this, perhaps, released under "revenge mode" malware, check out [7]Internet Storm Center's summary, and [8]know know your enemy, hopefully not until next month again! **UPDATE :** You can actually

go through another post in order to update yourself with some [9]recent malware developments.

Technorati tags : [10]malware, [11]Nyxem

1.

<https://photos1.blogger.com/blogger/1933/1779/1600/NyxemLatLonBig.0.jpg>

2. <http://www.f-secure.com/weblog/>



3. <http://ddanchev.blogspot.com/2006/01/malware-future-trends.html>
4. [http://www.f-secure.com/v-descs/nyxem\\_e.shtml](http://www.f-secure.com/v-descs/nyxem_e.shtml)
5. <http://www.f-secure.com/v-descs/nyxem.shtml>
6. <http://www.f-secure.com/weblog/#00000799>
7. <http://isc.sans.org/diary.php?storyid=1067>
8. <http://cme.mitre.org/data/list.html#24>
9. <http://ddanchev.blogspot.com/2006/02/recent-malware-developments.html>

148

10. <http://technorati.com/tag/malware>
11. <http://technorati.com/tag/Nyxem>

149

### **What search engines know, or may find out about us? (2006-02-03 15:33)**

Today, CNET's staff did an outstanding job of finding out [1]what major search companies retain about their users.

AOL, Google, Microsoft and Yahoo! respond on very well researched questions!

Whatever you do, just don't sacrifice innovation and trust in the current services for misjudged requests at

the first place from my point of view.

At the bottom line, differentiate your [2]Private Searches Versus Personally Identifiable Searches, consider visiting

[3]Root.net, [4]and [5]control your [6]Clickstream. You can also go through [7]Eric Goldman's comments on the

[8]issue and his [9]open letter regarding Search Engines and China.

As a matter of fact, I have just came across a very [10]disturbing fact that I compare with initiatives to [11]mine blogs for [12]marketing research, [13]EPIC has the details on its front page. It was about time a private entity comes up

with the idea given the potential and usability of the idea. Could such a concept spot, or actually seek for cyber

dissidents in restrictive regimes with the idea to [14]actually reach them, besides mining for extremists' data? I

really hope so!

Technorati tags:

[15]Privacy, [16]search engine, [17]Google, [18]Yahoo, [19]MSN, [20]AOL

1. [http://news.com.com/2102-1025\\_3-6034626.html?tag=st.util.print](http://news.com.com/2102-1025_3-6034626.html?tag=st.util.print)

2. <http://blog.searchenginewatch.com/blog/060123-074811>

3. <http://www.root.net/>

4. <http://www.techcrunch.com/2005/11/25/rootnets-lead-market/>

5. <http://www.swiss.ai.mit.edu/6.805/student-papers/fall95-papers/florey-privacy.html>
6. [http://www.mttl.org/volsix/Skok\\_art.html](http://www.mttl.org/volsix/Skok_art.html)
7. <http://blog.ericgoldman.org/>
8. [http://blog.ericgoldman.org/archives/2006/01/doj\\_fishes\\_for.htm](http://blog.ericgoldman.org/archives/2006/01/doj_fishes_for.htm)
9. [http://blog.ericgoldman.org/archives/2006/02/congress\\_search.htm](http://blog.ericgoldman.org/archives/2006/02/congress_search.htm)
10. <http://www.epic.org/privacy/choicepoint/acxiominternet.pdf>
11. <http://www.lwcresearch.com/filesfordownloads/SAPCRMvsSiebel.pdf>
12. <http://www.umbrialistens.com/>
13. <http://www.epic.org/>
14. <http://ddanchev.blogspot.com/2006/01/anonymity-or-privacy-on-internet.html>
15. <http://technorati.com/tag/Privacy>
16. <http://technorati.com/tag/search+engine>
17. <http://technorati.com/tag/Google>
18. <http://technorati.com/tag/Yahoo>
19. <http://technorati.com/tag/MSN>

20. <http://technorati.com/tag/AOL>

150

### **The current state of IP spoofing (2006-02-06 10:01)**

A week ago, I came across a great and distributed initiative to map the distribution of spoofable clients and networks

- the [1]ANA Spoofer Project, whose modest sample of 1100 clients, 500 networks and 450 ASes can still be used

to make informed judgements on the overall state of [2]IP Spoofing. I once posted some thoughts on "[3]How to

secure the Internet" where I was basically trying to emphasize on the fact that securing critical infrastructure by evaluating how hardened to attacks it really is, can be greatly improved as a concept. What if that infrastructure

is secured, but the majority of Internet communications remain in plain-text, and are easily spoofable, which I

find as one of the biggest current weaknesses. If you can spoof there's no accountability, and you can even get

DDoSed by [4]gary7.nsa.gov, isn't it? (in the original [5]Star Trek series, Gary Seven was the covert operative who

returned from the future to fix sabotage to the United States' first manned rocket to the moon moments before lift off).

On the other hand, according to Gartner [6]IPSec will be dead by 2008, but I feel this is where its peak and matu-

urity would actually be reached. IPv4 will evolve to IPv6, therefore IPSec will hopefully be an inseparable of the Internet.

## **So what's the bottom line so far?**

- 366 million spoofable IP addresses out of 1.78 billion
- 43,430 spoofable netblocks
- 4700 spoofable ASes out of 18450
- [7]NAT's and [8]XP SP2's make their impact

The higher the population the scarier the numbers for sure! I have always believed in distributed computing

and the power of the collective intelligence of thousands of people out there. Be it integrating powerful features

whose results are freely available to the public through OEM agreements or whatsoever, I feel in the future more

vendors will start taking advantage of their customers' base for

How you can contribute? [9]Pick up your client, start spoofing, but make sure your actions don't raise some-

one's eyebrows, even though you simply wanted to contribute, that's just a couple of packets to a university's server

that's looking forward to receiving them this time :)

[10]Dshield.org - the Distributed Intrusion Detection System is a very handy and useful [11]OSINT tool that is

obviously [12]being used by the NSA as well (check out the Internet Storm Center's [13]post on this, and the

[14]photo itself) UPDATE : Cryptome also featured fancy pictures from the [15]NSA's Threat Operations Wizardry.

What is your opinion on the current state of IP Spoofing on the web and the fact how handy this insecurity comes to

DDoS attacks? What should be done from your point of view to tackle the problem on a large scale?

**You can also consider going through many other distributed concepts :**

[16]The original DES Cracker Project

[17]DJohn - Distributed John

[18]Bob the Butcher distributed password cracker

[19]Seti at Home

[20]ForNet : A Distributed Forensics Network

[21]Pandora - Distributed Multirole Monitoring System

[22]FLoP - distributed Snort sensor

[23]DNSA - DNS auditing tool

151

[24]Despoof - anti packet spoofing

**As well as read more info on IP Spoofing, Distributed concepts and related tools :**

[25]IP Spoofing - An Introduction

[26]Distributed Tracing of Intruders

[27]Distributed Phishing Attacks

[28]MAC Distributed Security

[29]IPv6 Distributed Security(draft)

[30]Distributed Firewalls

[31]Web Spoofing

[32]The threats of distributed cracking

Technorati tags:

[33]security, [34]information security, [35]spoofing,  
[36]IPSec, [37]IPv6, [38]distributed

1. <http://spoofer.csail.mit.edu/>
2. [http://en.wikipedia.org/wiki/IP\\_spoofing](http://en.wikipedia.org/wiki/IP_spoofing)
3. <http://ddanchev.blogspot.com/2006/01/how-to-secure-internet.html>
4. <http://grc.com/dos/drDOS.htm>
5. <http://www.startrek.com/startrek/view/series/TOS/>
6. <http://www.techworld.com/security/news/index.cfm?NewsID=5173>
7. [http://en.wikipedia.org/wiki/Network\\_address\\_translation](http://en.wikipedia.org/wiki/Network_address_translation)
8. <http://www.microsoft.com/windowsxp/sp2/default.mspx>
9. <http://spoofer.csail.mit.edu/#software>
10. <http://www.dshield.org/>

11. <http://en.wikipedia.org/wiki/OSINT>
12. <http://www.washingtonpost.com/wp-dyn/content/article/2006/01/26/AR2006012601990.html>
13. <http://isc.sans.org/diary.php?storyid=1097>
14. <http://www.washingtonpost.com/wp-srv/photo/postphotos/orb/asection/2006-01-27/4.htm>
15. <http://cryptome.org/wiz/nsa-wizard.htm>
16. [http://www.eff.org/Privacy/Crypto/Crypto\\_misc/DESCracker/](http://www.eff.org/Privacy/Crypto/Crypto_misc/DESCracker/)
17. <http://www.ktulu.com.ar/en/djohn.php>
18. <http://packetstorm.linuxexposed.com/filedesc/bob-the-butcher-0.5.7.tar.html>
19. <http://setiathome.ssl.berkeley.edu/>
20. <http://isis.poly.edu/kulesh/research/pubs/mmm-acns-2003.pdf>
21. <http://pandoramon.sourceforge.net/>
22. <http://www.geschke-online.de/FLoP/>
23. <http://www.packetfactory.net/projects/dnsa/>
24. [http://www.bindview.com/Services/RAZOR/Utilities/Unix\\_Linux/despoof\\_readme.cfm](http://www.bindview.com/Services/RAZOR/Utilities/Unix_Linux/despoof_readme.cfm)
25. <http://www.securityfocus.com/infocus/1674>



26. <http://www.cs.ucdavis.edu/research/tech-reports/1995/CSE-95-2.pdf>
27. <http://www.cs.columbia.edu/wrfis/serendipity/uploads/phishing-5.pdf>
28. [http://grouper.ieee.org/groups/802/15/pub/2002/May02/02221r1P802-15\\_TG4-MAC-Distributed-Security-Proposal.ppt](http://grouper.ieee.org/groups/802/15/pub/2002/May02/02221r1P802-15_TG4-MAC-Distributed-Security-Proposal.ppt)
29. <http://www3.ietf.org/proceedings/04aug/slides/saag-2.pdf>
30. <http://www.cs.columbia.edu/~smb/papers/distfw.pdf>
31. <http://www.cs.princeton.edu/sip/pub/spoofing.pdf>
32. <http://www.swiss.ai.mit.edu/6.805/student-papers/fall97-papers/twyman-cracking.html>
33. <http://technorati.com/tag/security>

152

34. <http://technorati.com/tag/information+security>
35. <http://technorati.com/tag/spoofing>
36. <http://technorati.com/tag/IPSec>
37. <http://technorati.com/tag/IPv6>
38. <http://technorati.com/tag/distributed>

153

**Hacktivism tensions (2006-02-07 10:08)**

It was about time the freedom of the press and the democratic nature of joking with politicians takes its hit. But

why with spiritual leaders? The contradictory [1]Muhammad cartoons sparked a lot of [2]anger, and with the recent

[3]tentions in France all we needed was a [4]hacktivism activity from angry muslims. Remember how the [5]China

vs U.S cyberwar was [6]sparked [7]due to the death of a Chinese pilot crashing into an [8]AWACS that was sort of

"keeping it quiet"?

Zone-H is reporting on [9]massive defacements of Danish sites, and if you take the time to go through the reported

reasons you'll find out that :

*"political reasons"*

*"just for fun"*

*"I just want to be the best defacer"*

*"revenge against that web site"*

*"patriotism"*

tend to dominate. As far as defacements as concerned, in one of my previous posts "[10]FBI's 2005 Computer Crime

Survey - what's to consider?" you can see that according to the report, organizations lost approximately **\$10,395M**

due to web site defacements. Moreover, in some of my previous research on [11]Cyberterrorism I've indicated the use

of script kiddies for [12]PSYOPS and how such defacements have a favorable psychologic effect on future initiatives.

And while they have the motivation to deface, I wonder would someone strike back and under what justification?

Technorati tags:

[13]security, [14]information security, [15]defacement, [16]Zone-H, [17]hacktivism, [18]cyberterrorism, [19]Muham-mad cartoons, [20]hacking, [21]Denmark

1. <http://cryptome.org/muhammad.htm>
2. <http://news.bbc.co.uk/1/hi/world/europe/4670370.stm>
3. <http://cryptome.org/fr-riot/fr-riot-01.htm>
4. <http://en.wikipedia.org/wiki/Hacktivism>
5. [http://news.bbc.co.uk/hi/english/world/asia-pacific/newsid\\_1322000/1322839.stm](http://news.bbc.co.uk/hi/english/world/asia-pacific/newsid_1322000/1322839.stm)
6. <http://www.vitalsecurity.org/2006/01/first-hacker-world-war.html>
7. <http://www.astalavista.com/index.php?section=directory&linkid=6113>
8. [http://en.wikipedia.org/wiki/Airborne\\_warning\\_and\\_control\\_system](http://en.wikipedia.org/wiki/Airborne_warning_and_control_system)
9. <http://www.zone-h.org/en/news/read/id=205987/>
10. <http://ddanchev.blogspot.com/2006/01/fbis-2005-computer-crime-survey-whats.html>

11. <http://ddanchev.blogspot.com/2005/12/cyberterrorism-dont-stereotype-and-its.html>
12. [http://en.wikipedia.org/wiki/Psychological\\_operations](http://en.wikipedia.org/wiki/Psychological_operations)
13. <http://technorati.com/tag/security>
14. <http://technorati.com/tag/information+security>
15. <http://technorati.com/tag/defacement>
16. <http://technorati.com/tag/Zone-H>
17. <http://technorati.com/tag/hacktivism>
18. <http://technorati.com/tag/cyberterrorism>
19. <http://technorati.com/tag/Muhammad+cartoons>
20. <http://technorati.com/tag/hacking>
21. <http://technorati.com/tag/Denmark>

154

### **Security Awareness Posters (2006-02-07 13:35)**

Security is all about awareness at the bottom line. The better you understand it, the higher your chance of "survival", and hopefully progress!

Enjoy the following collections of witty and amusing security awareness posters :

[1]1, [2]2, [3]3 (you may also be interested in going through my talk on security policies and awareness with [4]K

Rudolph from Native Intelligence as well), [5]4, [6]5, [7]6, [8]7, [9]8.

Technorati tags:

[10]security, [11]information security, [12]security training,  
[13]security education

1. <http://members.impulse.net/~sate/posters.html>
2. [http://www.wasc.noaa.gov/wrso/posters/Security\\_Awareness\\_Posters1.htm](http://www.wasc.noaa.gov/wrso/posters/Security_Awareness_Posters1.htm)
3. <http://nativeintelligence.com/posters/security-posters.asp>
4. [http://www.windowsecurity.com/articles/Security\\_Talk1.html](http://www.windowsecurity.com/articles/Security_Talk1.html)
5. <http://www.iwar.org.uk/comsec/resources/ia-awareness-posters/>
6. [http://www.iupui.edu/~dmstest/Natl\\_Cybersecurity\\_Posters/FINAL\\_POSTERS/Full\\_Size\\_JPEGs/](http://www.iupui.edu/~dmstest/Natl_Cybersecurity_Posters/FINAL_POSTERS/Full_Size_JPEGs/)
7. <http://www.ussecurityawareness.org/highres/security-awareness.html>
8. <http://www.noticebored.com/html/posters.html>
9. <http://www.angelfire.com/tx/CZAngelsSpace/Security.html>
10. <http://technorati.com/tag/security>
11. <http://technorati.com/tag/information+security>
12. <http://technorati.com/tag/security+training>
13. <http://technorati.com/tag/security+education>

## **A top level espionage case in Greece (2006-02-08 15:14)**

Starting shortly after the Olympic games in 2004 and up to March 2005, the mobile phones of : Prime Minister Costas

Caramanlis, minister of foreign affairs, defense, public order and justice, top military officials, a number of journalists, and human rights activists (hmm?) [1]have been tapped [2]by an unknown party though the installation of "[3]spy

software" (that's too open topic) , mind you, Vodafone's central system, and were diverted to a pay-as-you-go mobile phone.

At the bottom line, who's behind it? Interested parties within the Greek government, or external ones? To

me this is the job of a [4]dead [5]insider's job or someone who had the incentive to Vodafone's security, which

I doubt. Though, it is disturbing how easily these mobile numbers could be obtained as the majority of media

representitives already have them! My point is that you should count them as the weakest link, besides accessing

a [6]mobile provider's database and other sources. **UPDATE** : [7]Vodafone's statement **UPDATE 2** : [8]Cryptome featured more info on the [9]The Greek illegal wiretapping scandal: some translations and resources.

Another recent spy case was the [10]rock transmitter found in a Moscow park and while the [11]Russian president

Putin is cheering the discovery and keeping it diplomatic, the [12]FSB (a [13]successor to the KGB) is taking a note on

this one. You can actually go through a [14]collection of videos and references on the case.

I guess it's the silence that's most disturbing in the "Silent War".

Technorati tags :

[15]security, [16]information security, [17]espionage, [18]Intelligence, [19]Greece, [20]Insider

1. <http://www.cnn.com/2006/WORLD/europe/02/06/greece.tapping.reut/>
2. [https://web.archive.org/web/20061026092427/http://www.ekathimerini.com/4dcgi/\\_w\\_articles\\_politics\\_100004\\_06/02/2006\\_66053](https://web.archive.org/web/20061026092427/http://www.ekathimerini.com/4dcgi/_w_articles_politics_100004_06/02/2006_66053)
3. <http://ddanchev.blogspot.com/2006/01/malware-future-trends.html>
4. [http://www.mpa.gr/article.html?doc\\_id=565920](http://www.mpa.gr/article.html?doc_id=565920)
5. <http://ddanchev.blogspot.com/2005/12/insiders-insights-trends-and-possible.html>
6. [http://www.epic.org/privacy/iei/attachment\\_a.pdf](http://www.epic.org/privacy/iei/attachment_a.pdf)
7. <http://www.vodafone.gr/live1/extp.jsp?type=prrel&prid=10467&lang=1&langSTR=en>
8. <http://cryptome.org/>

9. <http://homes.esat.kuleuven.be/~gdanezis/intercept.html>
10. <http://www.rian.ru/photolents/20060124/43153045.html>
11. <http://www.mosnews.com/news/2006/01/25/putinspies.shtml>
12. <http://www.fsb.ru/smi/remark/2006/060122-1.html>
13. [http://ddanchev.blogspot.com/2006/01/security\\_quotes-fsb-successor-to-kgb.html](http://ddanchev.blogspot.com/2006/01/security_quotes-fsb-successor-to-kgb.html)
14. <http://www.4law.co.il/ukspy2.htm>
15. <http://technorati.com/tag/security>
16. <http://technorati.com/tag/information+security>
17. <http://technorati.com/tag/espionage>
18. <http://technorati.com/tag/Intelligence>
19. <http://technorati.com/tag/Greece>
20. <http://technorati.com/tag/Insider>

156

### **The War against botnets and DDoS attacks (2006-02-09 15:44)**

In one of my previous posts talking about [1]botnet herders I pointed out how experiments tend to dominate, and

while [2]botnets protection is still a buzz word, major security vendors are actively working on product line extensions.



DDoS attacks are the result of successful botnet, and so are the root of the problem besides the [3]distributed

concept. Techworld is reporting that [4]McAfee is launching a "bot-killing system", from the article :

*"Unlike conventional DDoS detection systems based on the statistical analysis of traffic, the first layer of the new Advanced Botnet Protection (ABP) intrusion prevention system (IPS) uses a proxy to pass or block packet traffic dependent on whether or not it is "complete". "*

The best thing is that it's free, the bad thing is that it may give their customers a "false sense of security", that is, while the company is actively working on retaining its current customers, I feel "SYN cookies" and their concept has been around for years. Moreover, using a service provided by a company whose core competencies have nothing to

do with DDoS defense can be tricky. Companies worth mentioning are [5]Arbor Networks, and [6]Cisco's solutions,

besides the many other alternative and flexible ways of dealing with DDoS attacks.

In my research research on the [7]Future trends of Malware, I pointed out some of the trends related to botnets and

DDoS attacks, namely, **DDoS extortion, DDoS on demand/hire**, and with the first legally prosecuted case of [8]offering botnet access on demand, it's a [9]clear indication that of where things are going. Defense against frontal attacks isn't cost-effective given that at the bottom line the costs to maintain the site outpace the revenues generated for the time, hard dollars disappear, soft ones as reputation remain the same.

[10]My advice is to take into consideration the possibility to outsource your problem, and stay away from product

line extensions, and I think it's that very simple. A differentiated service on fighting infected nodes is being offered by Sophos, namely the [11]Zombie Alert, which makes me wonder why the majority of AV vendors besides them haven't

come up with an alternative given the data their sensor networks are able to collect? Moreover, should such a service

be free, would it end up as a licensed extension to be included within the majority of security solutions, and can a

motivated system administrators successfully detect, block, and isolate zombie traffic going out of the network(I think

yes!)?

As far as botnets are concerned, there were even speculations on using "[12]Skype to control botnets", now who would want to do that, and under what reason given the current approaches for controlling botnets, isn't the use of

cryptography or security through obscurity("talkative bots", stripping IRCds) the logical "evolution" in here?

Something else worth mentioning is the trend of how [13]DoS attacks got totally replaced by DDoS ones, my point is

that the first can be a much more sneaky one and easily go beneath the radar, compared to a large scale DDoS attack.

A single packet can be worth more than an entire botnets population, isn't it?

How do you think DDoS attacks should be prevented, active defense such as the solutions mentioned, or proactive

solutions? What do you think?

You can also go through other resources dealing with DDoS attacks and possible solutions to the problem :

[14]Dave Dittrich's DDoS attacks and protection page

[15]Recommendations for the Protection against Distributed Denial-of-Service Attacks in the Internet

[16]Botz-4-Sale: Surviving Organized DDoS Attacks That Mimic Flash Crowds

[17]Defense Against DoS/DDoS Attacks

[18]DDoS: Undeniably a global Internet problem looking for a global solution

[19]Scalable Protecting Against DDoS and Worm Attacks

[20]An Analysis of Using Reflectors An Analysis of Using Reflectors

157

[21]Attacking DDoS at the Source

[22]A Taxonomy of DDoS Attacks and DDoS Defense Mechanisms

[23]A Survey of DDoS Defense Mechanisms

[24]A summary of DoS/DDoS prevention, Monitoring and Mitigation Techniques in a Service Provider Environment

[25]Experience in fighting DDoS attacks

[26]Distributed Defense Against DDoS Attacks

[27]On the Effectiveness of DDoS Attacks on Statistical Filtering

[28]The Spamhaus Don't Route or Peer List (DROP)

[29]The Prolexic Zombie Report

Technorati tags :

[30]security, [31]information security, [32]malware,  
[33]botnets, [34]DDoS, [35]McAfee, [36]Sophos,  
[37]AntiVirus

1. <http://ddanchev.blogspot.com/2006/01/what-are-botnet-herds-up-to.html>

2. <http://en.wikipedia.org/wiki/Botnet>

3. <http://mixter.void.ru/protecting.txt>

4. <http://www.techworld.com/security/news/index.cfm?RSS&NewsID=5326>

5. <http://www.arbor.net/>

6. [http://www.cisco.com/en/US/netsol/ns615/networking\\_solutions\\_sub\\_solution.html](http://www.cisco.com/en/US/netsol/ns615/networking_solutions_sub_solution.html)

7. <http://ddanchev.blogspot.com/2006/01/malware-future-trends.html>

8. <http://edition.cnn.com/2006/TECH/internet/01/23/hacker.ap/>

9. <http://news.findlaw.com/hdocs/docs/cyberlaw/usanchetaind.pdf>
10. [https://web.archive.org/web/20061026092427/http://photos1.blogger.com/blogger/1933/1779/1600/sophos\\_zombie\\_alert\\_service.9.png](https://web.archive.org/web/20061026092427/http://photos1.blogger.com/blogger/1933/1779/1600/sophos_zombie_alert_service.9.png)
11. <http://www.sophos.com/products/es/zombiealert/>
12. <http://ddanchev.blogspot.com/2006/01/skype-to-control-botnets.html>
13. [http://en.wikipedia.org/wiki/Denial-of-service\\_attack](http://en.wikipedia.org/wiki/Denial-of-service_attack)
14. <http://staff.washington.edu/dittrich/misc/ddos/>
15. [http://www.iwar.org.uk/comsec/resources/dos/ddos\\_en.htm](http://www.iwar.org.uk/comsec/resources/dos/ddos_en.htm)
16. [http://www.akamai.com/en/resources/pdf/technical\\_publications/Botz4SaleSurvivingOrganizedDDoSAttacksThatMimicFlashCrowds.pdf](http://www.akamai.com/en/resources/pdf/technical_publications/Botz4SaleSurvivingOrganizedDDoSAttacksThatMimicFlashCrowds.pdf)
17. [http://www.infosecwriters.com/text\\_resources/pdf/Defense\\_DoS.pdf](http://www.infosecwriters.com/text_resources/pdf/Defense_DoS.pdf)
18. <http://www.ripe.net/ripe/meetings/ripe-41/tutorials/eof-ddos.pdf>
19. <https://web.archive.org/web/20061026092427/http://www.cs.purdue.edu/nsi/ftn-report.pdf>

20.

<https://web.archive.org/web/20061026092427/http://download.securityfocus.com/library/reflectors.CCR.01.pdf>

f

21.

<https://web.archive.org/web/20061026092427/http://www.eecs.umich.edu/~msim/Bibliography/DoSAttack/attackin>

[g-ddos-at-the-source.pdf](#)

22.

[https://web.archive.org/web/20061026092427/http://www.la.sr.cs.ucla.edu/ddos/ucla\\_tech\\_report\\_020018.pdf](https://web.archive.org/web/20061026092427/http://www.la.sr.cs.ucla.edu/ddos/ucla_tech_report_020018.pdf)

23.

[https://web.archive.org/web/20061026092427/http://webfealib.fea.aub.edu.lb/proceedings/2004/SRC-ECE-39.p](https://web.archive.org/web/20061026092427/http://webfealib.fea.aub.edu.lb/proceedings/2004/SRC-ECE-39.pdf)

[df](#)

24.

<https://web.archive.org/web/20061026092427/http://www.sans.org/rr/whitepapers/intrusion/1212.php>

25.

<https://web.archive.org/web/20061026092427/http://www.secure.org/presentations/ddos/COLT-SwiNOG9-ExpDD>

[oS-NF-v1.pdf](#)

26.

[https://web.archive.org/web/20061026092427/http://www.cis.udel.edu/~sunshine/publications/udel\\_tech\\_report](https://web.archive.org/web/20061026092427/http://www.cis.udel.edu/~sunshine/publications/udel_tech_report)

[\\_2005-02.pdf](#)

27.

<https://web.archive.org/web/20061026092427/http://www.comp.nus.edu.sg/~liqm/publications/DDoS.pdf>

158

28.

<https://web.archive.org/web/20061026092427/http://www.spamhaus.org/DROP/>

29.

<https://web.archive.org/web/20061026092427/http://www.prolexic.com/zr/>

30.

<https://web.archive.org/web/20061026092427/http://technorati.com/tag/security>

31.

<https://web.archive.org/web/20061026092427/http://technorati.com/tag/information+security>

32.

<https://web.archive.org/web/20061026092427/http://technorati.com/tag/malware>

33.

<https://web.archive.org/web/20061026092427/http://technorati.com/tag/botnets>

34.

<https://web.archive.org/web/20061026092427/http://technorati.com/tag/DDoS>

35.

<https://web.archive.org/web/20061026092427/http://technorati.com/tag/DDoS>

[ati.com/tag/McAfee](http://ati.com/tag/McAfee)

36.

<https://web.archive.org/web/20061026092427/http://technorati.com/tag/Sophos>

37.

<https://web.archive.org/web/20061026092427/http://technorati.com/tag/AntiVirus>

159

### **Who needs nuclear weapons anymore? (2006-02-09 16:29)**

Excluding [1]Iran and the potential of its nuclear program (no country [2]that bans music should have such a power!),

perhaps I should rephrase - who can actually use them nowadays, are they just a statement of power, does flexibility and beneath the radar concepts matter? I feel they do.

I just came across a news article from January on a new [3]EMP warhead test, and while there have been

speculations/or movie plots that [4]Electromagnetic Pulse Weapons could be used by [5]terrorists, I find this a bit of

exaggerated statement that actually seeks further investment in current development of the concept I guess. I feel

that compared to symmetric warfare, [6]asymmetric warfare as a concept has greatly evolved during the years, and

in today's interconnected society, military powers could be easily balanced. What's else to mention is the



"cooperation" between the parties on which I came across in a [7]report on Nuclear Electromagnetic Pulse, as of June 9, 2005, namely :

*"If we really wanted to hurt you with no fear of retaliation, we would launch an SLBM," which if it was launched in a submarine at sea, we really would not know for certain where it came from. "We would launch an SLBM, we would*

*detonate a nuclear weapon high above your country, and we would shut down your power grid and your*

*communications for 6 months or so." The third-ranking communist was there in the country. His name is Alexander*

*Shurbanov, and he smiled and said, "And if one weapon would not do it, we have some spares." I think the number of those spares now is something like 6,000 weapons."*

*"the Russians had developed weapons that produced 200 kilovolts per meter. Remember, the effects in Hawaii were judged to be the result of five kilovolts per meter. So this is a force about 200 times higher. The Russian generals said that they believed that to be several times higher than the hardening that we had provided for our military platforms that they could resist EMP."*

160

*"Chinese military writings described EMP as the key to victory and described scenarios where EMP is used against U.S.*

*aircraft carriers in the conflict over Taiwan." So it is not like our potential enemies do not know that this exists. The Soviets had very wide experience with this, and there is a lot*

*of information in the public domain relative to this. "A survey of worldwide military and scientific literature sponsored by the commission," that is the commission that*

*wrote this report, "found widespread knowledge about EMP and its potential military utility including in Taiwan,*

*Israel, Egypt, India, Pakistan, Iran, and North Korea."*

Still there's hope for preserving the global state of security instead of fuelling its insecurity :

*"In 2004, the EMP Commission met with very senior Russian officers, and we showed that on the sign. They warned that the knowledge and technology to develop what they called super EMP weapons had been transferred to North*

*Korea and that North Korea could probably develop these weapons in the near future, within a few years. The*

*Russian officers said that the threat that would be posed to global security by a North Korean armed with super EMP*

*weapons was, in their view, and I am sure, Mr. Speaker, in your view and mine, unacceptable."*

[8]Foreign views of Electromagnetic Pulse (EMP) Attack reveals further details on other nations' ambitions etc.

Perhaps one of the most famous commitments towards EMP is the [9]The Trestle Electromagnetic Pulse Simulator

that can also be seen at [10]Google Maps, still, in my opinion it's a defensive initiative for an offensive purpose :(



[11]

Extending the topic even further, [12]The Space Warfare arms race has been an active policy of key world's leaders

for decades, and that's not good. The U.S, Russia and China as the main players are fuelling the growth in one way or

other due to believing in perhaps :

- that the other sides are actively developing such capabilities, and they are, because they think the opposite =>

arms race

- growing trend towards [13]asymmetric warfare
- cost-effectiveness compared to building a multimillion nuclear submarine as a statement of power?

In my opinion space warfare would directly influence everyone down here on Earth, and scenarios such as :

- [14]satellites [15]jamming
- [16]space SIGING
- hijacking?
- destroying

could become normal. [17]Space is already getting crowded, if I were to forget one of my favourite quotes "[18]But I guess I'd say if it is just us... seems like an awful waste of space". On the other, and in respect to securing critical infrastructure on Earth :) I find recent initiatives such as the [19]Cyber Storm exercise more PR, than relevance

oriented, my point is that how come you expect to have the [20]critical infrastructure secured, when a [21]global

overload in traffic would again deny service, a critical one.

My point is that, the Internet as the most pervasive and cost effective tool is often utilized for sensitive both,

commercial, government and military operations, attacking the Internet affects pretty much everyone. Excluding the

overall shift towards [22]network-centric warfare and you've got a problem given commercial and public IP networks

are used to handle the [23]enormous bandwidth needed for sensitive operations.

To sum up, go through the following [24]War Quotes, and perhaps consider how major problems on Earth stop major

innovations in [25]Space. I feel War is not a solution, but an excuse that should never be said! I know this post tried

to combine several different issues, but I think given IP is at the bottom line, my readers wouldn't mind :) What's

your attitude on Space Warfare arms race? Is it real, and how do you picture the future developments in here?

162

More resources on **Electromagnetic Pulse Weapons**, **Space Warfare** and **Network-Centric Warfare** are also available at :

[26]High Altitude Electromagnetic Pulse (HEMP) and High Power Microwave (HPM) Devices: Threat Assessments

[27]The Effects Nuclear Weapons

[28]ELECTROMAGNETIC PULSE – (House of Representatives - June 21, 2005)

[29]Preliminary Findings of the Commission to Assess the Threat from EMP

[30]Communications Electronic Warfare and the Digitised Battlefield

[31]The Implementation of Network-Centric Warfare

[32]Complexity Theory and Network Centric Warfare

[33]On Space Warfare

[34]Warfare in Space

[35]Space Systems Survivability

[36]Developments in Military Space: Movement toward space weapons?

[37]Weapons in Space: Silver Bullet or Russian Roulette?

[38]From Cold War to Asymmetric Warfare

[39]Four Myths about Space Power

[40]China as a Military Space Competitor

1. <http://en.wikipedia.org/wiki/Iran>

2. [http://news.bbc.co.uk/2/hi/middle\\_east/4543720.stm](http://news.bbc.co.uk/2/hi/middle_east/4543720.stm)

3. <http://www.strategypage.com/htmw/htairw/articles/20060111.aspx>

4. [http://en.wikipedia.org/wiki/Electromagnetic\\_pulse](http://en.wikipedia.org/wiki/Electromagnetic_pulse)
5. <http://ddanchev.blogspot.com/2006/01/cyberterrorism-recent-developments.html>
6. [http://en.wikipedia.org/wiki/Asymmetric\\_warfare](http://en.wikipedia.org/wiki/Asymmetric_warfare)
7. <http://cryptome.org/bartlett-060905.txt>
8. [http://www.endtimesreport.com/EMP\\_attack.html](http://www.endtimesreport.com/EMP_attack.html)
9. <http://www.brook.edu/FP/projects/nucwcost/trestle.htm>
10. <http://maps.google.com/maps?q=Albuquerque,+NM&ll=35.029811,-106.557770&spn=0.005246,0.007693&t=k&hl=en>
11. [https://web.archive.org/web/20061026092427/http://photos1.blogger.com/blogger/1933/1779/1600/hf\\_tech\\_ewarf\\_are\\_050111\\_01.2.jpg](https://web.archive.org/web/20061026092427/http://photos1.blogger.com/blogger/1933/1779/1600/hf_tech_ewarf_are_050111_01.2.jpg)
12. [http://en.wikipedia.org/wiki/Space\\_warfare](http://en.wikipedia.org/wiki/Space_warfare)
13. [http://en.wikipedia.org/wiki/Asymmetric\\_warfare](http://en.wikipedia.org/wiki/Asymmetric_warfare)
14. <https://web.archive.org/web/20061026092427/http://www.gyre.org/news/related/Satellites/Satellite+Jamming>
15. [http://users.ox.ac.uk/~daveh/Space/Military/milspace\\_sigint.html](http://users.ox.ac.uk/~daveh/Space/Military/milspace_sigint.html)
16. <http://www.nro.gov/>
17. <http://eyeball-series.org/satspy/satspy-eyeball.htm>

18. <http://www.imdb.com/title/tt0118884/>

163

19.

[http://www.washingtontechnology.com/news/1\\_1/daily\\_news/27877-1.html](http://www.washingtontechnology.com/news/1_1/daily_news/27877-1.html)

20. <http://ddanchev.blogspot.com/2006/01/how-to-secure-internet.html>

21. <http://www.ists.dartmouth.edu/library/120.pdf>

22. <http://www.vodium.com/goto/oft/incw.asp>

23.

<http://www.californiaspaceauthority.org/images/pdfs/040831-milsatcom-anderson.pdf>

24. <http://quotes.prolix.nu/War/>

25. <http://www.space.com/>

26. <http://www.fas.org/man/crs/RL32544.pdf>

27.

<http://www.princeton.edu/~globsec/publications/effects/effects11.pdf>

28.

[http://www.bartlett.house.gov/SupportingFiles/documents/EMP\\_Speech\\_June\\_21\\_2005.pdf](http://www.bartlett.house.gov/SupportingFiles/documents/EMP_Speech_June_21_2005.pdf)

29. <http://empcreport.ida.org/3militaryVGversionJuly.pdf>

30.

<http://www.defence.gov.au/army/lwsc/Publications/wp%20116.pdf>

31. [http://www.oft.osd.mil/library/library\\_files/document\\_387\\_NC\\_W\\_Book\\_LowRes.pdf](http://www.oft.osd.mil/library/library_files/document_387_NC_W_Book_LowRes.pdf)
32. [http://www.dodccrp.org/publications/pdf/Moffat\\_Complexity.pdf](http://www.dodccrp.org/publications/pdf/Moffat_Complexity.pdf)
33. <http://www.maxwell.af.mil/au/au/aupress/Books/Lupton/lupton.pdf>
34. <http://space.au.af.mil/books/oberg/ch06.pdf>
35. [http://space.au.af.mil/primer/space\\_systems\\_survivability.pdf](http://space.au.af.mil/primer/space_systems_survivability.pdf)
36. <http://www.cdi.org/pdfs/space-weapons.pdf>
37. <http://www.cdi.org/pdfs/Hitchens-April2002-silver-bullet.pdf>
38. <http://www.stimson.org/wos/pdf/space1.pdf>
39. <http://carlisle-www.army.mil/usawc/Parameters/03spring/elhefnaw.pdf>
40. <http://www.gwu.edu/~spi/spaceforum/China.pdf>

164



**Recent Malware developments (2006-02-13 16:43)**



In some of my February's streams :) "[1]The War against botnets and DDoS attacks" and "[2]CME - 24 aka Nyxem, and who's infected?" I covered some of the recent events related to [3]malware trends in the first months of 2006.

This is perhaps the perfect time to say a big thanks to everyone who's been expressing ideas, remarks and thoughts

on my malware research. While conducting the research itself I realized that I simply cannot include everything I

want it, as I didn't wanted to release a book to have its content outdated in less than an year, but a "stick to the big picture" representation of the things to come. The best part is that while keeping daily track of the trends and trying to compile a summary to be released at the end of the year, many more concepts that I didn't include come to my

mind, so I feel I'll have enough material for a quality summary and justification of my statements. So what are some

of the recent developments to keep in mind?

A lot of buzz on the [4]CME-24 front, [5]and I [6]feel quite a lot of time was spent on speculating on the in-

fectected population out of a web counter whose results weren't that very accurate as originally though. And as vendors

closely cooperated to build awareness on the destructive payload, I think that's the first victory for 2006, no windows

of opportunity The best is that CAIDA patiently waited until the buzz is over to actually come up with [7]reliable

statistics on Nyxem.

[8]

It's rather quiet on the AV radars' from the way I see it, and quickly going

through F-Secure's, Kaspersky's (seem to be busy analyzing code, great real-time stats!), Symantec's I came across

the similarities you can feel for yourself in "the wild" :)

[9]Symantec's ThreatCon is normal, what's interesting to note is [10]VirusTotal's flood of detected WMF's, which is perhaps a consequence of the \*known\* [11]second vulnerability.

James Ancheta's case was perhaps the first known and so nicely documented on [12]botnet power on [13]

[14]demand. Recently, a botnet, or the participation in such [15]shut down a hos-

pital's network, more over I think StormPay didn't comply with a [16]DDoS extortion attempt during the weekend?

[17]Joanna Rutkowska provided more insights on stealth malware in her research ([18]slides, [19]demo) about

*"about new generation of stealth malware, so called Stealth by Design (SbD) malware, which doesn't use any of*

*the classic rootkit technology tricks, but still offers full stealth. The presentation also focuses on limitations of the current anti-rootkit technology and why it's not useful in fighting SbD malware. Consequently, alternative method for compromise [20]*

*detection is advocated in this presentation, Explicit Compromise*

*Detection (ECD), as well as the challenges which Independent Software Vendors encounter when trying to implement*

*ECD for Windows systems - I call it Memory Reading Problem (MRP). "*

How sound is the possibility of [21]malware heading towards the BIOS anyway? An "[22]Intelligent P2P worm's

activity" that I just across to also deserves to be mentioned, the concept is great, still the authors have to figure out 165

how to come up with legitimate file sizes for multimedia files if they really want to fake its existence, what do you think on this?

Some recent research and articles worth mentioning are, [23]Kaspersky's Malware - Evolution : October - De-

cember 2005 outlines the possibilities for [24]cryptoviral extortion attacks, 0days vulnerabilities, and [25]how the

WMF bug got purchased/sold for \$4000. There's also been quite a lot of [26]new trojans analyzed by third-party

researchers, and among the many recent articles that made me an impression are "[27]Malicious Malware: attacking

the attackers, part 1" and [28]part 2, from the article :

*"This article explores measures to attack those malicious attackers who seek to harm our legitimate systems.*

*The proactive use of exploits and bot networks that fight other bot networks, along with social engineering and*

*attacker techniques are all discussed in an ethical manner."*

[29]Internet worms and IPv6 [30]has nice points, still I wish there were only network based worms to bother

about. Besides all I've [31]missed [32]important [33]concepts [34]in various commentaries, did you? Malware is still

vulnerabilities/social engineering attacks split at least for the last several months, still the [35]increased corporate and home IM usage will inevitable lead to many more security threats to worry about. Web platform worms such as

[36]MySpace and [37]Google's AdSense Trojan, are [38]slowly gaining grounds as a Web 2.0 concept, so virus or IDS

[39]signatures are to look for, try both!

During January, David Aitel [40]reopened the subject of beneficial worms out of [41]Vesselin Bontchev's re-

search on "[42]good worms". While I have my [43]reservations on such a concept that would have to do with

patching mostly the way I see it, could exploiting a vulnerability in a piece of malware by considered useful some

day, or could a network mapping worm launched in the wild act as an early response system on mapped targets

that could end up in a malware's "hitlist"? And I also think the alternative to such an approach going beyond the network level is Johnny Long's ([44]recent chat with him) [45]Google Dorks Hacking Database, you won't need to

try to map the unlimited IPv6 address space looking for preys. Someone will either do the job for you, or with the

time, [46]transparency in [47]IPv6, one necessary for [48]segmented and targeted attacks will be [49]achieved as well.

Several days ago, Kaspersky released their [50]summary for 2005, nothing ground breaking in here compared

to previous research on [51]how the WMF vulnerability was purchased/sold for \$4000 :) but still, it's a very compre-

hensive and in-depth summary of 2005 in respect to the variables of a malware they keep track of. I recommend you

to go through it. What made me an impression?

- on average, **6368 malicious programs detected by month**

- **+272 % Trojan-Downloaders** 2005 vs 2004

- **+212 % Trojan-Dropper** 2005 vs 2004

- **+413 % Rootkit** 2005 vs 2004

- During 2005, on average **28 new rootkits a month**

- [52]IM worms **32 modifications per month**

- [53]IRC worms are on **-31 %**

166



- P2P worms are on **-43 %**, the best thing is that Kaspersky labs also shares my opinion on the reason for the decline,

P2P busts and general prosecutions for file-sharing. What's also interesting is to mention is the recent ruling in a

district court in Paris on the "[54]legality of P2P" in France and the charge of 5 EUR per month for access to P2P, but for how long? :) P2P [55]filesharing isn't illegal and if you cannot come up with a way to release your multimedia

content online, don't bother doing at all. In previous chats I had with [56]Eric Goldman, he also makes some

[57]very good points on the topic.

- **+68 % Exploit**, that is [58]software vulnerabilities and the use of exploits both known or 0day's with the idea to easily exploit targeted PC, though I'm expecting the actual percentage to be much higher

- Internet banking malware reached a record **402 % growth** rate by the end of 2005 The Trojan.Passwd is a very good example, it clearly indicates that it is written for financial gains. E-banking can indeed prove dangerous sometimes,

and while I'm not being a paranoid in here, I'd would recommend you go through Candid's well written "[59]Threats

to Consider when doing E-banking" paper

- A modest growth from 22 programs per month in 2004 to 31 in 2005 on the [60]Linux malware front

I feel today's malware scene is so vibrant that it's getting more and more complex to keep track of possible

propagation vectors, ecosystem here and there, and mostly [61]communicating what's going on to the general

public(actually this one isn't).

## **What's to come and what drives the current growth of malware?**

- money!

- the [62]commercialization of the market for software vulnerabilities, where we have [63]the first underground

purchase of the WMF exploit, so have software vulnerabilities always been the currency of trade in the security

world or they've started getting the necessary attention recently?

- is stealth malware more than an issue compared to utilizing 0day vulnerabilities, and is retaining current zombie

PCs a bigger priority than to infecting new ones?

- business competitors, enemies, unethical individuals are actively seeking for undetected pieces of malware coded

especially for their needs, these definitely go [64]beneath the sensors

- [65]Ancheta's case is a clear indication of a working Ecosystem from my point of view, that goes as high as to

provide after-sale services such as DDoS strength consultations and 0day malware on demand

[66]

To sum up, [67]malware tends to look so sneaky when spreading and zoomed out :) I

167

originally came across the [68]VisualComplexity project in one of my previous posts on [69]visualization. Feel I've missed something that's worth mentioning during the last two months? Than consider expanding the discussion!

You can also consider going through the following resources related to malware :

[70]Semantics-Aware Malware Detection

[71]Enabling Worm and Malware Investigation Using Virtualization

[72]Botnet Detection and Response - The Network is the Infection

[73]Fileprint analysis for Malware Detection

[74]Back to the Future: A Framework for Automatic Malware Removal and System Repair

[75]Assessing your Malware Exposure with Snort

[76]Truman - The Reusable Unknown Malware Analysis Net

[77]The Malcode Analyst Pack

[78]Nepenthes - malware collecting and visualizing tool

[79]Browser Appliance Virtual Machine

[80]Mwcollect - a distributed malware collector network

Technorati tags:



[81]security, [82]information security, [83]malware,  
[84]antivirus, [85]botnets, [86]kaspersky

1. <http://ddanchev.blogspot.com/2006/02/war-against-botnets-and-ddos-attacks.html>
2. <http://ddanchev.blogspot.com/2006/02/cme-24-aka-nyxem-and-whos-infected.html>
3. <http://ddanchev.blogspot.com/2006/01/malware-future-trends.html>
4. <http://cme.mitre.org/data/list.html#24>
5. <http://www.lurhq.com/blackworm-stats.html>
6. <http://www.f-secure.com/weblog/archives/archive-022006.html#00000800>
7. <http://www.caida.org/analysis/security/blackworm/>
8. [http://photos1.blogger.com/blogger/1933/1779/1600/virus\\_total\\_february\\_2006.0.png](http://photos1.blogger.com/blogger/1933/1779/1600/virus_total_february_2006.0.png)
9. <https://tms.symantec.com/>
10. [http://www.virustotal.com/flash/estadisticas\\_en.html](http://www.virustotal.com/flash/estadisticas_en.html)
11. <http://www.microsoft.com/technet/security/advisory/913333.mspx>
12. <http://news.findlaw.com/hdocs/docs/cyberlaw/usanchetaind.pdf>

13. [http://photos1.blogger.com/blogger/1933/1779/1600/f-secure\\_virus\\_statistics\\_february\\_2006.png](http://photos1.blogger.com/blogger/1933/1779/1600/f-secure_virus_statistics_february_2006.png)
14. <https://web.archive.org/web/20061026092427/http://news.findlaw.com/hdocs/docs/cyberlaw/usanchetaind.pdf>
15. [http://seattletimes.nwsources.com/html/localnews/2002798414\\_botnet11m.html](http://seattletimes.nwsources.com/html/localnews/2002798414_botnet11m.html)
16. [http://news.netcraft.com/archives/2006/02/10/payment\\_gateway\\_stormpay\\_battling\\_sustained\\_ddos\\_attack.html](http://news.netcraft.com/archives/2006/02/10/payment_gateway_stormpay_battling_sustained_ddos_attack.html)
17. <http://invisiblethings.org/>
18. [http://rootkit.com/redirect.php?http://invisiblethings.org/papers/rutkowska\\_bhffederal2006.pdf](http://rootkit.com/redirect.php?http://invisiblethings.org/papers/rutkowska_bhffederal2006.pdf)
19. <http://rootkit.com/redirect.php?http://invisiblethings.org/papers/rutkowska-bhffed2006-demos.rar>
20. [http://photos1.blogger.com/blogger/1933/1779/1600/kaspersky\\_virus\\_watch\\_february\\_2006.0.png](http://photos1.blogger.com/blogger/1933/1779/1600/kaspersky_virus_watch_february_2006.0.png)
21. [http://www.ngssoftware.com/jh\\_bhff2006.pdf](http://www.ngssoftware.com/jh_bhff2006.pdf)
- 168
22. <http://dustinbrewer.com/index.php>
23. <http://www.viruslist.com/en/analysis?pubid=178619907>

24. <http://www.cryptovirology.com/cryptovfiles/cryptovirologyfaqver1.html>
25. <http://ddanchev.blogspot.com/2006/01/was-wmf-vulnerability-purchased-for.html>
26. [http://www.megasecurity.org/files\\_archive/files012006.html](http://www.megasecurity.org/files_archive/files012006.html)
27. <http://www.securityfocus.com/infocus/1856>
28. <http://www.securityfocus.com/infocus/1857>
29. <http://www.cs.columbia.edu/~smb/papers/v6worms.pdf>
30. [http://www.schneier.com/blog/archives/2006/02/internet\\_worms.html](http://www.schneier.com/blog/archives/2006/02/internet_worms.html)
31. <http://www.cs.berkeley.edu/~nweaver/warhol.html>
32. <http://www.cs.columbia.edu/~smb/papers/fnat.pdf>
33. <http://www.cis.upenn.edu/~anagnost/papers/nasr-worm05.pdf>
34. <http://tennis.ecs.umass.edu/~czou/research/routingWorm-techreport.pdf>
35. <http://ddanchev.blogspot.com/2006/01/whats-potential-of-im-security-market.html>
36. <http://namb.la/popular/tech.html>
- 37.

<http://www.techshout.com/internet/2005/27/a-trojan-horse-program-that-targets-google-ads-has-been-detected-by-an-indian-web-publisher/>

38. <http://www.securityfocus.com/columnists/364>

39. <http://ddanchev.blogspot.com/2006/01/why-relying-on-virus-signatures-simply.html>

40. <http://www.securityfocus.com/news/11373>

41. <http://www.people.frisk-software.com/~bontchev/>

42. <http://www.people.frisk-software.com/~bontchev/papers/goodvir.html>

43. [http://www.wormblog.com/2004/11/the\\_myth\\_of\\_the.html](http://www.wormblog.com/2004/11/the_myth_of_the.html)

44. <http://www.astalavista.com/index.php?section=directory&linkid=6182>

45. <http://johnny.ihackstuff.com/index.php?module=prodreviews>

46. <http://ddanchev.blogspot.com/2005/12/ip-cloaking-and-competitive.html>

47. [http://www.intellectualicebergs.org/archives/intice\\_08\\_060129.mp3](http://www.intellectualicebergs.org/archives/intice_08_060129.mp3)

48. <http://ddanchev.blogspot.com/2006/01/malware-future-trends.html>

49. <http://www.sockpuppet.org/tqbf/log/2006/02/ipv6-will-mark-it-hard-for-worms-to.html>

50. <http://www.viruslist.com/en/analysis?pubid=178949694>
51. <http://ddanchev.blogspot.com/2006/01/was-wmf-vulnerability-purchased-for.html>
52.  
<https://web.archive.org/web/20061026092427/http://ddanchev.blogspot.com/2006/01/whats-potential-of-im-security-market.html>
53.  
<https://web.archive.org/web/20061026092427/http://www.astalavista.com/media/directory/uploads/e84fd6eabeffa188c493d27d1d94f27b.pdf>
54.  
[http://www.theregister.co.uk/2006/02/08/france\\_legalises\\_p2p/](http://www.theregister.co.uk/2006/02/08/france_legalises_p2p/)
55. <http://www.geocities.com/SoHo/Suite/2003/mp3.jpg>
56. <http://www.ericgoldman.org/>
57.  
[http://www.astalavista.com/media/archive1/newsletter/issue\\_19\\_2005.pdf](http://www.astalavista.com/media/archive1/newsletter/issue_19_2005.pdf)
58. <http://ddanchev.blogspot.com/2006/01/was-wmf-vulnerability-purchased-for.html>
59.  
[http://www.trojan.ch/paper/ThreatsToOnlineBanking\\_Candid\\_Wueest.pdf](http://www.trojan.ch/paper/ThreatsToOnlineBanking_Candid_Wueest.pdf)
60. <http://linuxmafia.com/~rick/faq/index.php?page=virus>

61. <http://cme.mitre.org/>
62. <http://ddanchev.blogspot.com/2005/12/0bay-how-realistic-is-market-for.html>
63. <http://ddanchev.blogspot.com/2006/01/was-wmf-vulnerability-purchased-for.html>
64. <http://www.cs.cmu.edu/~bethenco/cipart2005.pdf>
65. <http://news.findlaw.com/hdocs/docs/cyberlaw/usanchetaind.pdf>
66. <http://photos1.blogger.com/blogger/1933/1779/1600/1000-worms.jpg>
67. <http://www.e-things.org/worms/>
68. <http://www.visualcomplexity.com/vc/>
- 169
69. <http://ddanchev.blogspot.com/2006/01/visualization-intelligence-and.html>
70. <http://www.astalavista.com/index.php?section=directory&linkid=5419>
71. <http://www.cs.purdue.edu/homes/dxu/CERIAS.ppt>
72. <http://www.caida.org/projects/oarc/200507/slides/oarc0507-Dagon.pdf>
73. <http://www1.cs.columbia.edu/~wl318/papers/wormpaper200>

[5.pdf](#)

74. <http://www.cs.ucdavis.edu/research/tech-reports/2005/CSE-2005-6.pdf>

75. <http://www.kgb.to/malware.html>

76. <http://www.lurhq.com/truman/>

77. <http://labs.iddefense.com/labs-software.php?show=8>

78. <http://nepenthes.sourceforge.net/>

79. <http://www.vmware.com/vmtn/vm/browserapp.html>

80. <http://www.mwcollect.org/>

81. <http://technorati.com/tag/security>

82. <http://technorati.com/tag/information+security>

83. <http://technorati.com/tag/malware>

84. <http://technorati.com/tag/antivirus>

85. <http://technorati.com/tag/botnets>

86. <http://technorati.com/tag/kaspersky>

170

### **Look who's gonna cash for evaluating the maliciousness of the Web? (2006-02-14 17:12)**

Two days ago, SecurityFocus ran an article "[1]Startup tries to spin a safer Web" introducing [2]SiteAdvisor :

*"A group of graduates from the Massachusetts Institute of Technology (MIT) aim to change that by crawling the Web*

*with hundreds, and soon thousands, of virtual computers that detect which Web sites attempt to download software*

*to a visitor's computer and whether giving out an e-mail address during registration can lead to an avalanche of spam.*

*The goal is to create a service that lets the average Internet user know what a Web site actually does with any*

*information collected or what a download will do to a computer, Tom Pinckney, vice president of engineering and*

*co-founder of the [3] start-up SiteAdvisor, said during a presentation at the [4] CodeCon conference here."*

The concept is simply amazing, and while it's been around for ages, it stills needs more acceptance from decision

makers that tend to stereotype on perimeter and antivirus defense only. Let's start from the basics, it is my opinion

that users do more surfing than downloading, that is, the Web and its insecurities represent a greater threat than

users receiving malware in their mailboxes or IMs. And not that they don't receive any, but I see a major shift

towards URL droppers, and while defacement groups are more than willing to [5]share these with phishers etc., a

URL dropper is easily getting replaced by an IP one, so you end up having infected PCs infecting others through

hosting and distributing the malware, so [6]sneaky, isn't it? My point is that initiatives such as crawling the web for



malicious sites, listing, categorizing and updating their status is a great, both security, and business sound

opportunity. The way you know the bad neighbourhoods around your town, in that very same way you need a

visualization to assist in research, or act as a security measure, and while its hard to map the Web and keep it up to

date, I find the idea great!

So what is [7]SiteAdvisor up to? Another build-to-flip startup? I doubt so as I can almost feel the smell of quality

entrepreneurship from [8]MIT's graduates, of course, given they assign a CEO with business background :) APIs,

plugins, already tested the majority of popular sites according to them, and it's for free, at least to the average

Internet user who's virtual "word of mouth" will help this project get the scale and popularity necessary to see it licensed and included within current security solutions. They simply cannot test the entire Web, and I feel the

shouldn't even set it as an objective, instead map the most trafficked web sites or do so on-the-fly with the top 20

results from Google. I wonder how are downloads tested, are they run through VirusTotal for instance, and how

significant could a "push" approach from the end users, thus submitting direct links to malicious files found within to domain for automatic analysis, sound in here?

I think the usefulness of their idea could only be achieved with the cooperation/acquisition of a [9]leading search

engine, my point is that some of the project's downsides are the lack of on-the-fly ability(that would be like v2.0 and

a major breakthrough in respect to performance), how it's lacking the resources to catch up with Google on the

known web (25,270,000,000 according to them recently), how IP droppers instead of URL based ones totally ruin the

idea in real-life situations(it takes more efforts to register and maintain a domain, compared to using a zombie host's

capabilities to do the same, doesn't it?)

In one of my previous posts on [10]why you should aim higher than antivirus signatures protection only I mentioned

some of my ideas on *"Is client side sandboxing an [11] alternative as well, could and would a customer agree to act as a sandbox compared to the current(if any!) contribution of forwarding a suspicious sample? Would v2.0 constitute of*

*a [12] collective automated web petro in a PC's "spare time"?*

Crawling for malicious content and making sense of the approaches used in order to provide an effective solutions is

very exciting topic. As a matter of fact in one of my previous posts "[13]What search engines know, or may find

171

about us?" I mentioned about the existence of a project to [14]mine the Web for terrorist sites dating back to 2001.

And I'm curious on its progress in respect to the [15]current [16]threat of Cyberterrorism, I feel both, crawling for

malicious content and terrorist propaganda have a lot in common. Find the bad neighbourhoods, and have your

spiders do whatever you instruct them to do, but I still feel quality and in-depth overview would inevitably be

sacrificed for automation.

What do you think is its potential of web crawling for malicious content, and by malicious I also include harmful in

respect to Cyberterrorism [17]PSYOPS (I once came across a [18]comic PSYOPS worth reading!) techniques that I

come across on a daily basis? Feel [19]free to test any site you want, or browse through their [20]catalogue as well.

You can also find more info on the topic, and alternative crawling solutions, projects and Cyberterrorism activities

online here :

[21]A Crawler-based Study of Spyware on the Web

[22]Covert Crawling: A Wolf Among Lambs

[23]IP cloaking and competitive intelligence/disinformation

[24]Automated Web Patrol with HoneyMonkeys Finding Web Sites That Exploit Browser Vulnerabilities

[25]The Strider HoneyMonkey Project

[26]STRIDER : A Black-box, State-based Approach to Change and Configuration Management and Support

[27]Webroot's Phileas Malware Crawler

[28]Methoden und Verfahren zur Optimierung der Analyse von Netzstrukturen am Beispiel des AGN-Malware

Crawlers (in German)

[29]Jihad Online : Islamic Terrorists and the Internet

[30]Right-wing Extremism on the Internet

[31]Terrorist web sites courtesy of the [32]SITE Institute

[33]The HATE [34]Directory November 2005 update (very rich content!)

[35]Recruitment by Extremist Groups on the Internet

Technorati tags:

[36]security, [37]information security, [38]SiteAdvisor, [39]web crawler, [40]search engine, [41]cyberterrorism

1. <http://www.securityfocus.com/news/11376>
2. <http://www.siteadvisor.com/preview/>
3. <http://www.siteadvisor.com/>
4. <http://www.codecon.org/2006/>
5. <http://www.vnunet.com/vnunet/news/2149449/amd-forum-users-exposed-wmf>
6. <http://ddanchev.blogspot.com/2006/01/malware-future-trends.html>
7. <http://www.siteadvisor.com/preview/>
8. <http://www.mit.edu/>

9. <http://www.google.com/>
10. <http://ddanchev.blogspot.com/2006/01/why-relying-on-virus-signatures-simply.html>
11. <http://www.vmware.com/vmtn/vm/browserapp.html>
12. <http://research.microsoft.com/honeymonkey/>
13. <http://ddanchev.blogspot.com/2006/02/what-search-engines-know-or-may-find.html>
14. <http://www.epic.org/privacy/choicepoint/acxiominternet.pdf>
15. <http://ddanchev.blogspot.com/2006/01/cyberterrorism-recent-developments.html>
16. <http://ddanchev.blogspot.com/2005/12/cyberterrorism-dont-stereotype-and-its.html>
17. <http://en.wikipedia.org/wiki/PSYOPS>
18. <http://www.ep.tc/grenada/index.html>
- 172
19. <http://www.siteadvisor.com/preview/>
20. <http://www.siteadvisor.com/map/>
21. <http://www.cs.washington.edu/homes/gribble/papers/spycrawler.pdf>
22. <http://www.astalavista.com/index.php?section=directory&linkid=6104>

23. <http://ddanchev.blogspot.com/2005/12/ip-cloaking-and-competitive.html>
24. <ftp://ftp.research.microsoft.com/pub/tr/TR-2005-72.pdf>
25. <http://research.microsoft.com/HoneyMonkey/>
26. [http://research.microsoft.com/asia/dload\\_files/group/system/LISA.pdf](http://research.microsoft.com/asia/dload_files/group/system/LISA.pdf)
27. <http://www.webroot.com/>
28. [http://agn-www.informatik.uni-hamburg.de/papers/doc/studarb\\_rene\\_soller.pdf](http://agn-www.informatik.uni-hamburg.de/papers/doc/studarb_rene_soller.pdf)
29. [http://www.adl.org/internet/jihad\\_online.pdf](http://www.adl.org/internet/jihad_online.pdf)
30. <http://www.inach.net/content/Annual%20Report%20jugendschutz.pdf>
31. <http://siteinstitute.org/websites.html>
32. <http://siteinstitute.org/>
33. <https://web.archive.org/web/20061026092427/http://www.bcpl.net/~rfrankli/hatedir.htm>
34. <http://www.bcpl.net/~rfrankli/hatedir.pdf>
35. [http://firstmonday.org/issues/issue6\\_2/ray/index.html](http://firstmonday.org/issues/issue6_2/ray/index.html)
36. <http://technorati.com/tag/security>
37. <http://technorati.com/tag/information+security>

38. <http://technorati.com/tag/SiteAdvisor>
39. <http://technorati.com/tag/web+crawler>
40. <http://technorati.com/tag/search+engine>

41. <http://technorati.com/tag/cyberterrorism>

173

## **Detecting intruders and where to look for (2006-02-15 08:48)**

[1]CERT, just released their "[2]Windows Intruder Detection Checklist" from the article :

*"This document outlines suggested steps for determining whether your Windows system has been compromised.*

*System administrators can use this information to look for several types of break-ins. We also encourage you to*

*review all sections of this document and modify your systems to address potential weaknesses."*

I find it a well summarized checklist, perhaps the first thing that I looked up when going through it was the

[3]rootkits section given the topic. It does provide links to free tools, but I feel they could have extended to topic a little bit. Overall, consider going through it. Another checklist I recently came across is the "[4]11 things to do after a hack" and another quick summary on "[5]10 threats you probably didn't make plans for".

[6]Rootkits are gaining popularity, and with a reason - it takes more efforts to infect new victims instead of

keeping the current ones, at least from the way I see it. In one of my previous post "[7]Personal Data Security

Breaches - 2000/2005" I mentioned about a rootkit placed on a server at the [8]University of Connecticut on October



26, 2003, but wasn't detected until July 20, 2005, enough for auditing, detecting attackers and forensics? Well, not

exactly, still something else worth mentioning is the interaction between auditing, rootkits and forensics. There's

also been another reported event of using [9]rootkit technologies for DRM(Digital Right Management) purposes, not

on [10]CDs, but DVDs this time, so it's not enough that malware authors are utilizing the rootkit concept, but flawed

approaches from companies where we purchase our CDs and DVDs from, are resulting in more threats to deal with!

Check CERT's "[11]Windows Intruder Detection Checklist" and if interested, also go through the following re-

sources on rootkits and digital forensics :

[12]Windows rootkits of 2005, part one

[13]Windows rootkits of 2005, part two

[14]Windows rootkits of 2005, part three

[15]Malware Profiling and Rootkit Detection on Windows

[16]Timing Rootkits

[17]Shadow Walker - Raising The Bar For Windows Rootkit Detection - [18]slides

[19]When Malware Meets Rootkits

[20]Leave no trace - book excerpt

- [21]Database Rootkits
- [22]Rootkits and how to combat them
- [23]Rootkits Analysis and Detection
- [24]Concepts for the Stealth Windows Rootkit
- [25]Avoiding Windows Rootkit Detection
- [26]Checking Microsoft Windows Systems for Signs of Compromise
- [27]Implementing and Detecting Implementing and Detecting an ACPI BIOS Rootkit
- [28]Host-based Intrusion Detection Systems
- [29]Forensics Tools and Processes for Windows XP Clients
- [30]F.I.R.E - Forensic and Incident Response Environment Bootable CD
- [31]Forensic Acquisition Utilities
- [32]FCCU GNU/Linux Forensic Bootable CD 10.0
- [33]iPod Forensics :)
- [34]Forensics of a Windows system
- [35]First Responders Guide to Computer Forensics
- [36]Computer Forensics for Lawyers

174

Technorati tags:

[37]security, [38]information security, [39]forensics,  
[40]rootkit, [41]security breach, [42]CERT

1. <http://www.cert.org/>
2. [http://www.cert.org/tech\\_tips/WIDC.html](http://www.cert.org/tech_tips/WIDC.html)
3. [http://www.cert.org/tech\\_tips/WIDC.html#C1](http://www.cert.org/tech_tips/WIDC.html#C1)
4. [http://searchwindowssecurity.techtarget.com/generic/0,295582,sid45\\_gci1161209,00.html](http://searchwindowssecurity.techtarget.com/generic/0,295582,sid45_gci1161209,00.html)
5. [http://www.infosecwriters.com/text\\_resources/pdf/Ten\\_Threats\\_ABycroft.pdf](http://www.infosecwriters.com/text_resources/pdf/Ten_Threats_ABycroft.pdf)
6. <http://rootkit.com/>
7. <http://ddanchev.blogspot.com/2006/01/personal-data-security-breaches.html>
8. <http://www.uconn.edu/>
9. <http://www.f-secure.com/weblog/archives/archive-022006.html#00000810>
10. <http://www.sysinternals.com/blog/2005/10/sony-rootkits-and-digital-rights.html>
11. [http://www.cert.org/tech\\_tips/WIDC.html](http://www.cert.org/tech_tips/WIDC.html)
12. <http://www.securityfocus.com/infocus/1850>
13. <http://www.securityfocus.com/infocus/1851>
14. <http://www.securityfocus.com/infocus/1854>

15. [http://xcon.xfocus.org/archives/2005/Xcon2005\\_Shok.pdf](http://xcon.xfocus.org/archives/2005/Xcon2005_Shok.pdf)
16. [http://www.kd-team.com/papers/Timing\\_Rootkits.pdf](http://www.kd-team.com/papers/Timing_Rootkits.pdf)
17. [http://www.phrack.org/phrack/63/p63-0x08\\_Raising\\_The\\_Bar\\_For\\_Windows\\_Rootkit\\_Detection.txt](http://www.phrack.org/phrack/63/p63-0x08_Raising_The_Bar_For_Windows_Rootkit_Detection.txt)
18. <http://www.blackhat.com/presentations/bh-jp-05/bh-jp-05-sparks-butler.pdf>
19. <http://www.symantec.com/avcenter/reference/when.malware.meets.rootkits.pdf>
20. [http://searchsecurity.techtarget.com/searchSecurity/downloads/Hoglund\\_ch1.pdf](http://searchsecurity.techtarget.com/searchSecurity/downloads/Hoglund_ch1.pdf)
21. [http://www.red-database-security.com/wp/db\\_rootkits\\_us.pdf](http://www.red-database-security.com/wp/db_rootkits_us.pdf)
22. <http://www.viruslist.com/en/analysis?pubid=168740859>
23. <http://www.cert-in.org.in/training/29thmarch05/rootkits.pdf>
24. [http://www.invisiblethings.org/papers/chameleon\\_concepts.pdf](http://www.invisiblethings.org/papers/chameleon_concepts.pdf)
25. <http://www.geocities.com/embarbosa/bypass/bypassEPA.pdf>
26. [http://www.ucl.ac.uk/cert/win\\_intrusion.pdf](http://www.ucl.ac.uk/cert/win_intrusion.pdf)
27. [http://www.ngssoftware.com/jh\\_bh2006.pdf](http://www.ngssoftware.com/jh_bh2006.pdf)

28. <http://staff.science.uva.nl/~delaat/snb-2004-2005/p19/report.pdf>
29. <http://www.blackhat.com/presentations/bh-asia-02/bh-asia-02-leibrock.pdf>
30. <http://fire.dmzs.com/?section=main>
31. <http://users.erols.com/gmgarner/forensics/>
32. <http://www.lnx4n6.be/index.php>
33. [https://www.cerias.purdue.edu/tools\\_and\\_resources/bibtex\\_archive/archive/2005-13.pdf](https://www.cerias.purdue.edu/tools_and_resources/bibtex_archive/archive/2005-13.pdf)
34. [http://www.fistconference.org/data/presentaciones/forensics\\_ofawindowssystem.pdf](http://www.fistconference.org/data/presentaciones/forensics_ofawindowssystem.pdf)
35. [http://www.cert.org/archive/pdf/FRGCF\\_v1.3.pdf](http://www.cert.org/archive/pdf/FRGCF_v1.3.pdf)
36. [http://www.craigball.com/cf\\_vcr.pdf](http://www.craigball.com/cf_vcr.pdf)
37. <http://technorati.com/tag/security>
38. <http://technorati.com/tag/information+security>
39. <http://technorati.com/tag/forensics>
40. <http://technorati.com/tag/rootkit>
41. <http://technorati.com/tag/security+breach>
42. <http://technorati.com/tag/CERT>

## **A timeframe on the purchased/sold WMF vulnerability (2006-02-15 19:03)**

The **[1]WMF vulnerability and how it got purchased/sold for \$4000** was a major event during January, at least for

me as for quite some time the industry was in the twilight zone by not going through a recently released report. But

does this fact matters next to figuring out how to safeguard the security of your network/PC given the time it took

the vendor to first, realize that it's real, than to actually patch it? Something else that made me an impression is that compared to the media articles and my post, was I the only one interested in who bought, instead of who sold it?

So here's a short timeframe on how it made it to to the mainstream media :

**January 27** - Kaspersky are the first to mention the "purchase" in their **[2]research**

**January 30** I've started **[3]blowing the whistle** and **[4]friends** picked it up (even the guy that got so upset about it!) **January 31** Meanwhile, someone eventually **[5]breached AMD's forums** and started infecting its visitors!

**February 2** **[6]Microsoft Switzerland's Security** blog featured it

**February 2** **[7]LinuxSecurity.com** republished it

**February 2** **[8]DSLReports.com** picked it up

**February 2** Appeared at **[9]Slashdot**

**February 3 [10]OSIS.gov**(an unclassified network serving the intelligence community with **[11]open source intelligence**) picked it up :)

What's the conclusion? Take your time and read the reports thoroughly, cheer Kaspersky's team for their research?

For sure, but keep an eye on the **[12]Blogosphere** as well!

**Technorati tags :**

[13]security, [14]information security, [15]wmf vulnerability, [16]vulnerabilities, [17]Kaspersky

1. <http://ddanchev.blogspot.com/2006/01/was-wmf-vulnerability-purchased-for.html>
2. <http://www.viruslist.com/en/analysis?pubid=178619907>
3. <http://ddanchev.blogspot.com/2006/01/was-wmf-vulnerability-purchased-for.html>
4. <http://www.sahw.com/wp/archivos/2006/01/31/el-mercado-de-las-vulnerabilidades-0day/>
5. <http://www.vnunet.com/vnunet/news/2149449/amd-forum-users-exposed-wmf>
6. [http://blogs.technet.com/ms\\_schweiz\\_security\\_blog/archive/2006/02/02/418615.aspx](http://blogs.technet.com/ms_schweiz_security_blog/archive/2006/02/02/418615.aspx)
7. <http://www.linuxsecurity.com/content/view/121477?rdf>
8. <http://www.dslreports.com/forum/remark,15384516>

9. <http://it.slashdot.org/article.pl?sid=06/02/02/215210&from=rss>
10. <http://www.fas.org/irp/program/disseminate/osis.htm>
11. <http://en.wikipedia.org/wiki/OSINT>
12. <http://en.wikipedia.org/wiki/Blogosphere>
13. <http://technorati.com/tag/security>
14. <http://technorati.com/tag/information+security>
15. <http://technorati.com/tag/wmf+vulnerability>
16. <http://technorati.com/tag/vulnerabilities>
17. <http://technorati.com/tag/Kaspersky>

176

### **The end of passwords - for sure, but when? (2006-02-16 19:15)**

My first blog post "[1]How to create better passwords - why bother?!" back in December, 2005, tried to briefly summarize my thoughts and comments I've been making on the most commonly accepted way of identifying yourself

- passwords.

[2]Bill Gates did a commentary on the issue, note where, at the [3]RSA Conference, perhaps the company

that's most actively building awareness on the potential/need for two-factor authentication, or anything else but



using static passwords for various access control purposes. Moreover, it was again Bill Gates who wanted to

integrate the [4]Belgian eID card with MSN Messenger ([5]Anonymity or Privacy on the Internet?) Microsoft are

always reinventing the wheel, be it with [6]antivirus, or their [7]Passport service, and while they have the financial

obligations to any of their stakeholders, I feel it's a wrong approach on the majority of occasions.

What I wonder is, are they forgetting the fact that over 95 % of the PCs out there, run Microsoft Windows,

and not Vista, and how many would continue to do so polluting the Internet at the bottom line. My point is that MS's

constant rush towards "[8]the next big thing" doesn't actually provides them with the resources to tackle some of the current problems, at least in a timely manner. What do you think? What could Microsoft do to actually influence

the acceptance of [9]two-factor authentication, and moreover, [10]how feasible is [11]the concept at the bottom line?

### **Technorati tags :**

[12]security, [13]microsoft, [14]authentication, [15]passwords

1. <http://ddanchev.blogspot.com/2005/12/how-to-create-better-passwords-why.html>

2. [http://searchsecurity.techtarget.com/originalContent/0,289142,sid14\\_gci1166552,00.html](http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1166552,00.html)
3. <http://www.rsaconference.com/>
4. [http://www.theregister.co.uk/2005/02/01/msn\\_belgium\\_id\\_cards/](http://www.theregister.co.uk/2005/02/01/msn_belgium_id_cards/)
5. <http://ddanchev.blogspot.com/2006/01/anonymity-or-privacy-on-internet.html>
6. [http://blog.washingtonpost.com/securityfix/2006/02/microsoft\\_antispyware\\_deleting\\_1.html](http://blog.washingtonpost.com/securityfix/2006/02/microsoft_antispyware_deleting_1.html)
7. <http://www.zdnet.co.uk/comment/other/0,39020682,39183062,00.htm>
8. <http://www.microsoft.com/windowsvista/>
9. [http://en.wikipedia.org/wiki/Two-factor\\_authentication](http://en.wikipedia.org/wiki/Two-factor_authentication)
10. [http://www.schneier.com/blog/archives/2005/03/the\\_failure\\_of.html](http://www.schneier.com/blog/archives/2005/03/the_failure_of.html)
11. <http://ddanchev.blogspot.com/2006/01/security-threats-to-consider-when.html>
12. <http://technorati.com/tag/security>
13. <http://technorati.com/tag/microsoft>
14. <http://technorati.com/tag/authentication>

15. <http://technorati.com/tag/passwords>

177

**How to win 10,000 bucks until the end of March?  
(2006-02-17 13:45)**

[1]I feel that, in response to the recent event of how the  
[2]WMF vulnerability got purchased/sold for \$4000 (an  
[3]interesting timeframe as well), [4]iDefense are actively  
working on strengthening their market positioning - that  
is the maintain their pioneering position as a perhaps the  
first company to start paying vulnerability researchers for  
their discoveries.

The company recently [5]offered \$10,000 for the  
submission or a vulnerability that gets categorized as  
critical

in any of Microsoft's Security Bulletins. In the long-term,  
would vulnerability researchers be able to handle the

pressure put on them through such financial incentives, and  
keep their clear vision instead of sell their souls/skills?

What if someone naturally offers more, would money be the  
incentive that can truly close the deal, and is it just me

realizing how bad is it to commercialize the not so mature  
vuln research market, namely how this would leak all of  
its current weaknesses?

Consider going through some of my previous thoughts on  
the [6]emerging market for software/0day vulnera-

bilities as well and stay tuned for another recent discovery a dude tipped me on, thanks as a matter of fact!

Technorati tags:

[7]idefense, [8]vulnerabilities

1. <http://photos1.blogger.com/blogger/1933/1779/1600/dollars.jpg>
2. <http://ddanchev.blogspot.com/2006/01/was-wmf-vulnerability-purchased-for.html>
3. <http://ddanchev.blogspot.com/2006/02/timeframe-on-purchasedsold-wmf.html>
4. <http://idefense.com/>
5. <http://labs.idefense.com/vcp.php>
6. <http://ddanchev.blogspot.com/2005/12/0bay-how-realistic-is-market-for.html>
7. <http://technorati.com/tag/idefense>
8. <http://technorati.com/tag/vulnerabilities>

178



## **Smoking emails (2006-02-17 23:41)**

[1]

I just came across this, "[2]Morgan Stanley offers \$15M fine for e-mail violations" - from the article :

*" US investment bank Morgan Stanley will offer a settlement to the Securities and Exchange Commission (SEC),*

*agreeing in principle to pay a \$15 million fine for failing to preserve e-mail messages. The e-mail messages could*

*have provided useful evidence in several cases brought against the company. In one case, resulting in a \$1.58 billion judgement against the bank, a judge turned the burden of proof on Morgan Stanley after learning they had deleted*

*e-mails related to the case. However, Morgan Stanley has not yet presented the offer to the SEC nor is there a*

*guarantee the SEC will accept. The investment bank says it is fixing the problems that led to the erasure and is*

*pleading for leniency. "*

He, He, He!

179

You see, the email archiving market is about to top \$310M for 2005 according to the IDC, still one of the world's most powerful investment banks cannot seem to be able to comply with the requirements.

Lack of financial power - nope, lack of incentives - yep! The case reminds me of KPMG's tax shelters, [3]McAfee's fine

for accounting scam between 1998-2000, and the "[4]Smoking Emails" Admissible In \$1 Billion Enron-Related Chase Case".

Quit smoking emails, and take advantage of [5]MailArchiva - Open Source Email Archiving and Compliance.

Techorati tags :

[6]smoking gun, [7]investment banking, [8]compliance, [9]mailarchiva

1. <https://photos1.blogger.com/blogger/1933/1779/1600/smoking.jpg>

2. <https://draft.blogger.com/http://www.computerworld.com/securitytopics/security/recovery/story/0,10801,108687,00.html>

3. <http://www.techworld.com/security/news/index.cfm?RSS&NewsID=5098>

4. <http://www.law.com/jsp/article.jsp?id=1039054493212>

5. <http://openmailarchiva.sourceforge.net/>

6. <http://technorati.com/tag/smoking+gun>

7. <http://technorati.com/tag/investment+banking>

8. <http://technorati.com/tag/compliance>

9. <http://technorati.com/tag/mailarchiva>

180



## **DVD of the weekend - The Lone Gunmen (2006-02-17 23:47)**

[1]

The [2]Lone Gunmen on two double-sided discs, pure classic! In one of my chats with Roman Polesek, from [3]Hakin9,

he was wise enough to state the you cannot be a prophet in your own industry, simple, but powerful statement you should take into consideration.

Initiatives such as The Lone Gunmen, the [4]X-files, and [5]The Outer Limits have already proven useful, given someone listens! [6]For instance :

*" In a foreshadowing of the September 11, 2001 attacks, subsequent conspiracy theories, and the 2003 inva-*

*sion of Iraq, the plot of the March 4, 2001 pilot episode of the series depicts a secret U.S. government agency plotting to crash a Boeing 727 into the World Trade Center via remote control for the purpose of increasing the military*

*defence budget and blaming the attack on foreign "tin-pot dictators" who are "begging to be smart-bombed." This episode aired in Australia less than two weeks before the 9/11 attacks, on August 30. "*

Conspiracy theorists do have a lot to say, so don't ignore them, find the balance, and enjoy the series :)

You can also browse through some transcripts as well.

Technorati tags :

[7]conspiracy

1. <https://photos1.blogger.com/blogger/1933/1779/200/gunmen.0.jpg>
2. <http://www.thelonegunmen.com/>
3. <http://www.hakin9.org/en/>
4. <http://www.foxhome.com/xfiles8/>
5. <http://www.theouterlimits.com/>
6. [http://en.wikipedia.org/wiki/Lone\\_Gunmen](http://en.wikipedia.org/wiki/Lone_Gunmen)
7. <http://technorati.com/tag/conspiracy>

181

### **Chinese Internet Censorship efforts and the outbreak (2006-02-24 13:14)**

In some of my [1]January's Security Streams, I did some extensive blogging expressing my point of view on the

current [2]Internet censorship activities, and tried to emphasize on the country whose Internet population is about

to outpace the U.S one - China. In my posts "[3]China - the biggest black spot on the Internet's map", "[4]2006 =

1984?", "[5]Twisted Reality", you can quickly update yourself on some of the recent developments related to the topic, but what has changed ever since?



Government bodies such as the DoJ seem to favour the amount of data the most popular and [6]advanced

search engine Google holds and [7]tried to obtain information for the purpose of "social responsibility". What's more to consider are some of the [8]weak statements made, namely :

*"House Government Reform Committee Chairman Tom Davis (R-VA) has criticized Google for refusing to hand*

*search records over to the US Justice Department while cooperating with China in censoring certain topics. Justice*

*sought the records to bolster its case against a challenge to online anti-pornography laws, but Google refuses to*

*submit the records on privacy grounds. Davis does not expect a standoff between Google and the government, but*

*hopes an agreement can be reached, allowing Google to supply the records without frightening users that their*

*searches may be examined."*

and in case you're interested, some of my [9]comments, :

*"Is it just me or that must be sort of a black humour political blackmail given the situation?! First, and most of all, the idea of using search engines to bolster the online anti-pornography laws created enough debate for years of commentaries and news stories, and was wrong from the very beginning. Even if Google provide the data requested*

*it doesn't necessarily solve the problem, so instead of blowing the whistle without any point, sample the top 100*

*portals and see how they enforce these policies, if they do. As far as China is concerned, or actually used as a point of discussion, remember the different between modern communism, and democracy as a concept, the first is an excuse for the second, still, I feel it's one thing to censor, another to report actual activity to law enforcement. I feel alternative methods should be used, and porn "to go" is a more realistic threat to minors than the Net is to a certain extend, yet the Net remains the king of content as always."*

Google indeed issued a [10]statement, sort of excusing the censorship under the statement of "the time has

come to open ourselves to the Chinese market", and while their intentions make business sense, [11]the [12]out-

break [13]had [14]very positive consequences from my point of view - build more awareness and have the world's

eyes on the Chinese enforcement of censorship practices, but is it just China to blame given "Western" countries do censor as well, or is it China's huge ambitions of maintaining a modern communism in the 21st century that seem to

be the root of the problem?

[15]

In an article "[16]A day in the life of a Chinese Internet Police Officer" I read some time ago, you can clearly 182

see the motivation, but also come across the facts themselves : you cannot easily censor such a huge Internet population, instead, guidance instead of blocking, and self-regulation(that is limiting yourself with fear of prosecution) seem to be the current practice, besides [17]jailing

journalists! And while sometimes, you really need to come up

with a [18]creative topic worth writing about, [19]free speech is among the most important human rights at the bottom line.

[20]Chris Smith, Chairman of the House subcommittee that oversees Global Human Rights, proposed a discus-

sion draft "[21]The Global Online Freedom Act of 2006" " *to promote freedom of expression on the internet [and] to protect United States businesses from coercion to participate in repression by authoritarian foreign governments*". It is so "surprising" to find out that they are so interested in locating cyber-dissidents : "*U.S. search engine providers must transparently share with the U.S. Office of Global Internet freedom details of terms or parameters submitted by Internet-restricting countries.*" exactly the same way I mentioned in my previous "[22]Anonymity or Privacy on the Internet?" post.

Meanwhile, the [23]OpenNetInitiative also [24]released a [25]bulletin analyzing Chinese non-commercial web-

site registration regulation, giving even further details on the recent "you're being watched" culture that tries to cost-effectively deal with the issue of self-regulation :

" *In a report published last year, "[26] Internet Filtering in China: 2004-2005," ONI shared its research findings that China's filtering regime is the most extensive, technologically sophisticated, and broad-reaching Internet filtering system in the world. This new regulation does not rely on sophisticated filtering technology, but uses the threat of surveillance and legal sanction to pressure*

*bloggers and website owners into self-censorship. While savvy website*

*owners might thwart the registration requirement with relative ease, the regulation puts the vast majority of Chinese Internet users on notice that their online behaviour is being monitored and adds another layer of control to China's already expansive and successful Internet filtering regime. "*

Yet another recent research I came across is a university study that finds out that "[27]60 % Oppose Search

Engines Storing Search Behaviours", you can also consider the "[28]alternatives" if you're interested :) A lots to happen for sure, but it is my opinion that personalized search is the worst privacy time bomb a [29]leading search

engine should not be responsible for, besides open-topic data retention policies and not communicating an event

such as the DoJ's one, but complying with it right away, bad Yahoo!, bad MSN!

At the bottom line, Google's notifications of censored content(as of March, 2005 only, [30]excluding the pe-

riod before!), the general public's common sense on easily evaluating what's blocked and what isn't, and the

powerful digital rights fighting organizations that simultaneously increased their efforts to gain the maximum out of

the momentum seemed to have done a great job of building awareness on the problem. Still, having to live with the

booming wanna be "free market" Chinese economy, and the country's steadily climbing position as a major economic partner, economic sanctions, quotas, or real-life scenarios would remain science fiction.

183

Technorati tags :

[31]Privacy, [32]Anonymity, [33]Censorship, [34]China, [35]Search Engine

1. <http://ddanchev.blogspot.com/2006/01/januarys-security-streams.html>
2. [http://en.wikipedia.org/wiki/Censorship\\_in\\_cyberspace](http://en.wikipedia.org/wiki/Censorship_in_cyberspace)
3. <http://ddanchev.blogspot.com/2006/01/china-biggest-black-spot-on-internets.html>
4. <http://ddanchev.blogspot.com/2006/01/2006-1984.html>
5. <http://ddanchev.blogspot.com/2006/01/twisted-reality.html>
6. [http://www.google.com/advanced\\_search?hl=en](http://www.google.com/advanced_search?hl=en)
7. <http://ddanchev.blogspot.com/2006/01/feds-google-msns-reaction-and-how-you.html>
8. [http://www.gcn.com/vol1\\_no1/daily-updates/38097-1.html?CMP=OTC-RSS](http://www.gcn.com/vol1_no1/daily-updates/38097-1.html?CMP=OTC-RSS)
9. [http://www.astalavista.com/media/archive1/newsletter/issue\\_25\\_2006.pdf](http://www.astalavista.com/media/archive1/newsletter/issue_25_2006.pdf)

10. <http://googleblog.blogspot.com/2006/02/human-rights-caucus-briefing.html>
11. <http://userscripts.org/scripts/show/3070>
12. <http://www.freetibet.org/press/pr250106.html>
13. <http://news.bbc.co.uk/2/hi/asia-pacific/4712134.stm>
14. [http://www.excal.on.ca/index.php?option=com\\_content&task=view&id=1479&Itemid=2](http://www.excal.on.ca/index.php?option=com_content&task=view&id=1479&Itemid=2)
15. [http://photos1.blogger.com/blogger/1933/1779/1600/20060208\\_01.jpg](http://photos1.blogger.com/blogger/1933/1779/1600/20060208_01.jpg)
16. [http://www.zonaeuropa.com/20060208\\_1.htm](http://www.zonaeuropa.com/20060208_1.htm)
17. <http://cryptome.cn/cn-torture.htm>
18. <http://ddanchev.blogspot.com/2006/02/hacktivism-tensions.html>
19. <http://www.eff.org/br/>
20. <http://www.house.gov/chris-smith/>
21. [http://rconversation.blogs.com/rconversation/files/SMITNJ\\_094\\_XML.pdf](http://rconversation.blogs.com/rconversation/files/SMITNJ_094_XML.pdf)
22. <http://ddanchev.blogspot.com/2006/01/anonymity-or-privacy-on-internet.html>
23. <http://www.opennetinitiative.net/>
24. <http://releases.usnewswire.com/GetRelease.asp?id=61353>

25. <http://opennet.net/bulletins/011/>
26. [http://www.opennetinitiative.net/studies/china/ONI\\_China\\_Country\\_Study.pdf](http://www.opennetinitiative.net/studies/china/ONI_China_Country_Study.pdf)
27. <http://www.uconn.edu/newsmedia/2006/February/rel06011.html>
28. <http://ddanchev.blogspot.com/2006/01/still-worry-about-your-search-history.html>
29. <http://www.google.com/>
30. <http://www.google.com/support/bin/answer.py?answer=17795&topic=368>
31. <http://technorati.com/tag/Privacy>
32. <http://technorati.com/tag/Anonymity>
33. <http://technorati.com/tag/Censorship>
34. <http://technorati.com/tag/China>
35. <http://technorati.com/tag/Search+Engine>

184

### **Master of the Infected Puppets (2006-02-24 14:37)**

[1]In some of my previous posts, "[2]What are botnet herds up to?", "[3]Skype to control Botnets", "[4]The War against Botnets and DDoS attacks", and "[5]Recent Malware Developments", I was actively providing resources and updating my blog readers (thanks for the tips and the info sharing, I mean it!) related to one of the most relevant

[6]threats to the Internet ( more [7]trends and [8]bureaucracy ) - **Botnets**.

I recently came across a well researched [9]report giving a very in-depth overview and summary of important concepts related to Botnets. Recommended bed time reading, and here's an excerpt :

*"In this paper we begin the process of codifying the capabilities of malware by dissecting four widely-used Internet Relay Chat (IRC) botnet codebases. Each codebase is classified along seven key dimensions including botnet control mechanisms, host control mechanisms, propagation mechanisms, exploits, delivery mechanisms, obfuscation and deception mechanisms. Our study reveals the complexity of botnet software, and we discusses implications for defense strategies based on our analysis"*

Some of the findings that I also came across in my "[10]Malware - future trends" search worth mentioning

are :

- *"The overall architecture and implementation of botnets is complex, and is evolving toward the use of com-*

*mon software engineering techniques such as modularity."* Namely, no one is interested in [11]reinventing the wheel again, and the Simple Botnet/Malware Communication Protocol I've once mentioned (originally came across the



concept [12]here) could give the malware scene an impressive scale, but could it also put AV vendors and researchers

in favorable position where exploiting protocol weaknesses is more beneficial than current approaches?

- *"Shell encoding and packing mechanisms that can enable attacks to circumvent defensive systems are com-*

185

*mon. However, Agobot is the only botnet codebase that includes support for (limited) polymorphism"*

Smart! Mainly because of the fact that *" The malware delivery mechanisms used by botnets have implications*

*for network intrusion detection and prevention signatures. In particular, NIDS/NIPS benefit from knowledge of*

*commonly used shell codes and ability to perform simple decoding. If the separation of exploit and delivery becomes*

*more widely adopted in bot code (as we anticipate it will), it suggests that NIDS could benefit greatly by incorporating rules that can detect follow-up connection attempts. "*

*-"All botnets include a variety of sophisticated mechanisms for avoiding detection (e.g., by anti-virus software) once installed on a host system."*

Retention instead of acquisition of new zombies would tend to dominate from my point of view. Patching the

hosts themselves, [13]hiding presence, dealing with the easy to detect idle zombie's presence, TCP obfuscations,

tests for debuggers, are among the current methods used.

[14]

Botnets will continue to dominate due to their [15]concept and [16]potential for growth, and while monitor-

ing and doing active research is still feasible, encrypted communications as a logical development should also be

researched as a concept, but how many \*public\* IRC servers, if such are used, support SSL encryption?

Technorati tags :

[17]Security, [18]Information Security, [19]Malware, [20]Botnets

1.

<https://photos1.blogger.com/blogger/1933/1779/1600/master-of-puppets.jpg>

2. <http://ddanchev.blogspot.com/2006/01/what-are-botnet-herds-up-to.html>

3. <http://ddanchev.blogspot.com/2006/01/skype-to-control-botnets.html>

4. <http://ddanchev.blogspot.com/2006/02/war-against-botnets-and-ddos-attacks.html>

5. <http://ddanchev.blogspot.com/2006/02/recent-malware-developments.html>

186

6. <http://ddanchev.blogspot.com/2006/01/how-to-secure-internet.html>

7. <http://ddanchev.blogspot.com/2006/01/fbis-2005-computer-crime-survey-whats.html>
8. <http://ddanchev.blogspot.com/2006/01/to-report-or-not-to-report.html>
9. [http://www.cs.wisc.edu/~pb/botnets\\_final.pdf](http://www.cs.wisc.edu/~pb/botnets_final.pdf)
10. <http://ddanchev.blogspot.com/2006/01/malware-future-trends.html>
11. <http://ddanchev.blogspot.com/2006/01/skype-to-control-botnets.html>
12. <http://www.amazon.com/gp/product/0321304543/002-6251435-2774409?v=glance&n=283155>
13. <http://ddanchev.blogspot.com/2006/02/detecting-intruders-and-where-to-look.html>
14. [https://photos1.blogger.com/blogger/1933/1779/1600/encrypted\\_botnet\\_communications.jpg](https://photos1.blogger.com/blogger/1933/1779/1600/encrypted_botnet_communications.jpg)
15. <http://www.egghelp.org/>
16. <http://www.egghelp.org/tcl.htm>
17. <http://technorati.com/tag/Security>
18. <http://technorati.com/tag/Information+Security>
19. <http://technorati.com/tag/Malware>
20. <http://technorati.com/tag/Botnets>

## **Give it back! (2006-02-24 15:36)**

According to a recent article "[1]Secret program reclassifies documents" :

*"Researcher Matthew Aid has discovered a secret reclassification program that has moved thousands of declassified pages out of the National Archives and Records Administration's facility in Maryland. Some groups, such as George Washington University's Nation Security Archive, are fighting to end the program, arguing that the government has no right take back information it has published. The reclassification has been ongoing since 1999 as the Central Intelligence Agency, the Defense Intelligence Agency, and the Defense and Justice departments take back information they say had been inadvertently published. The National Security Archive describes some of the documents that have been reclassified as uninteresting and mundane."*

And from The National Security Archive :

*"Washington, D.C., February 21, 2006 - The CIA and other federal agencies have secretly reclassified over 55,000 pages of records taken from the open shelves at the National Archives and Records Administration (NARA), according to*

*[2] a report published today on the World Wide Web by the National Security Archive at George Washington University."*

[3]

[4]OSINT [5]has greatly evolved from President Nixon's remark in respect to the [6]CIA *"What use are they?"*

*They've got over 40,000 people over there reading newspapers."*, whereas Secrecy is a major weakness to the

national security of a country in a very complex way. I feel that sometimes, you need the average citizen's unbiased

opinion on a major issue, but I guess I'm not into politics, just figuring out what is going on at the bottom line!

More on Secrecy, Intelligence, Misc :

[7]Making Intelligence Accountable

[8]Why Spy? The Uses and Misuses of Intelligence (1996)

[9]Intelligence Analysis for Internet Security : Ideas, Barriers and Possibilities

[10]U.S. Electronic Espionage : A Memoir

[11]Terrorism prevention in Russia : one year after Beslan

[12]Crypto Law Survey

[13]Cryptome

[14]Project on Government Secrecy

[15]Shhh!!: Keeping Current on Government Secrecy

Technorati tags :

[16]Secrecy, [17]Intelligence

1. <http://www.fcw.com/article92379-02-21-06-Web&RSS=yes>
2. <http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB179/#report>
3. <http://www.prwatch.org/images/wmd.gif>
4. <http://en.wikipedia.org/wiki/OSINT>
5. <http://www.cia.gov/csi/studies/vol48no3/article05.html>
6. [http://www.cia.gov/csi/studies/Vol49no2/reexamining\\_the\\_distinction\\_3.htm](http://www.cia.gov/csi/studies/Vol49no2/reexamining_the_distinction_3.htm)
7. [http://www.dcaf.ch/handbook\\_intelligence/\\_publications.cfm](http://www.dcaf.ch/handbook_intelligence/_publications.cfm)
8. <http://www.cato.org/pubs/pas/pa-265.html>
9. <http://www.cert.org/archive/html/spie.html>
10. <http://jya.com/nsa-elint.htm>
11. <http://studies.agentura.ru/english/listing/terrorismprevention/>
12. <http://rechten.uvt.nl/koops/cryptolaw/>
13. <http://cryptome.org/>
14. <http://www.fas.org/sgp/>

15. <http://www.infoday.com/searcher/jan06/Gordon-Murnane.shtml>

16. <http://technorati.com/tag/Secrecy>

17. <http://technorati.com/tag/Intelligence>

189

### **One bite only, at least so far! (2006-02-24 16:21)**

[1]Apple's OS X has always been positioned as a juicy target even though it's market share is almost non-existent

compared to Microsoft's domination. And while converting iPod customers into MAC users hasn't shown any progress

so far and I doubt it would, malware authors are as always actively experimenting or diversifying the threatscape.

One question remains unclear, why would someone want to own a MAC, compared to owning hundreds of thousands

of Windows PCs out there? To me, it's not about achieving the scale necessary for a [2]Botnet, rather, experiment,

show that it's possible through POC releases, or basically start attacking the living in a safe heaven until for now, MAC

users.

Recently, an [3]OS X trojan appeared, [4]second (nice attitude from Apple on embracing the inevitable!), [5]one

[6]followed, and besides "worming" a vulnerability and experimenting with propagation methods, I don't really think it's the big trend everyone is waiting for, a standard

POC(Cabir), whose core function would empower a generation

of variants for years to come.

I just came across this from Trifinite's blog :

*"[7] Trifinite.groupmember [8] Kevin has published a [9] paper detailing the techniques he used in the development of the InqTana Bluetooth worm that targets vulnerable Mac OS X systems. There has been significant confusion*

*surrounding this worm, so here are some salient points:*

- The concurrent release of the OS X Leap.A and InqTana.A worms is coincidental*

- There is no conspiracy, AV vendors and Apple were notified about Kevin's progress in developing this worm in advance of making details publicly available*

- Both 10.3 and 10.4 systems are vulnerable until patched with APPLE-SA-2005-05-03 and APPLE-SA-2005-06-*

*08*

- InqTana prompts before infecting \*by design\*, Kevin was just trying to be nice, but the worm could easily*

*spread silently*

*Kevin's paper is available at [10]*

*<http://www.digitalmunition.com/InqTanaThroughTheEyes.txt>.*

*Comments can*



*be directed to the [11] BlueTraQmailing list. Our sympathies to those organizations who were affected by the*

*false-positive signatures published by overzealous AV companies."*

190

It clarifies a lot I think, mostly that, while architecture and OS popularity have a lot to do with security and incentives for attacks, *"InqTana.A itself has absolutely nothing to do with Leap.A. My work was done completely independent of the author of Leap. The day after I sent out queries to the AV companies about my code I was*

*shocked to see another OSX worm had already been in the news. While my worm sat in the mail spools of several AV*

*companies they were busy writing about the "First Trojan/Worm for OSX"."*

Leakage of IP, or I'm being a paranoid in here? [12]Wired also has some nice comments.

Technorati tags :

[13]Security, [14]Information Security, [15]Apple, [16]Malware, [17]Leap, [18]InqTana, [19]Anti Virus

1.

[http://photos1.blogger.com/blogger/1933/1779/1600/apple\\_virus.jpg](http://photos1.blogger.com/blogger/1933/1779/1600/apple_virus.jpg)

2. <http://ddanchev.blogspot.com/2006/02/war-against-botnets-and-ddos-attacks.html>

3. <http://www.securityfocus.com/brief/142>

4. <http://www.securityfocus.com/brief/143>
5. <http://www.f-secure.com/weblog/archives/archive-022006.html#00000819>
6. <http://www.viruslist.com/en/weblog>
7. [http://trifinite.org/trifinite\\_group.html](http://trifinite.org/trifinite_group.html)
8. [http://trifinite.org/trifinite\\_group\\_kevin.html](http://trifinite.org/trifinite_group_kevin.html)
9. <http://www.digitalmunition.com/InqTanaThroughTheEyes.txt>
10. <http://www.digitalmunition.com/InqTanaThroughTheEyes.txt>
11. <https://lists.trifinite.org/mailman/listinfo/bluetraq>
12. <http://www.wired.com/news/columns/0,70257-0.html>
13. <http://technorati.com/tag/Security>
14. <http://technorati.com/tag/Information+Security>
15. <http://technorati.com/tag/Apple>
16. <http://technorati.com/tag/Malware>
17. <http://technorati.com/tag/Leap>
18. <http://technorati.com/tag/InqTana>
19. <http://technorati.com/tag/Anti+Virus>

## **DVD of the Weekend - The Outer Limits - Sex And Science Fiction Collection (2006-02-25 20:35)**

*" A sextet of sci-fi tales opens with Alyssa Milano as a woman whose "close encounter" leaves her with an insatiable lust in "Caught in the Act"; the sole survivor of a nuclear holocaust gets some computer-generated companionship in*

*"Bits of Love," with Natasha Henstridge; Sofia Shinas is "Valerie 13," a robot whose emotions become all-too-human; a man who's lived his life onboard a mysterious spaceship meets his female counterpart in "The Human Operators,"*

*with Jack Noseworthy and Polly Shannon; a nerd becomes a ladies man via a high-tech "image enhancer" in "Skin Deep," with Antonio Sabato, Jr. and Adam Goldberg; and an alien plant becomes a deadly and*

*seductive "Flower Child," with Jud Taylor."*

[1]Get it, [2]find [3]out [4]more, and [5]listen to the wisdom from previous episodes.

1. <http://www.amazon.com/gp/product/B000068V9S/002-5192813-5250468?v=glance&n=130>

2. <http://www.theouterlimits.com/index2.html>

3. <http://www.innermind.com/outerlimits/>

4. [http://en.wikipedia.org/wiki/The\\_Outer\\_Limits](http://en.wikipedia.org/wiki/The_Outer_Limits)

5. <http://www.theouterlimits.com/downloads/index.html?controlvoices>

## **Get the chance to crack unbroken Nazi Enigma ciphers (2006-02-27 10:49)**

[1]Nice initiative I just came across to. From the "[2]M4 Message Breaking Project" :

*The M4 Project is an effort to break 3 original Enigma messages with the help of distributed computing. The*

*signals were intercepted in the North Atlantic in 1942 and are believed to be unbroken. Ralph Erskine has presented*

*the intercepts in a [3] letter to the journal Cryptologia. The signals were presumably enciphered with the four rotor Enigma M4 - hence the name of the project.*

*This project has officially started as of January 9th, 2006. You can help out by donating idle time of your com-*

*puter to the project. If you want to participate, please follow the client install instructions for your operating system:*

[4] *Unix Client Install*

[5] *Win98 Client Install*

[6] *Win2000 Client Install*

[7] *WinXP Home Client Install*

[8] *WinXP Pro Client Install*

The first message is already [9]broken as a matter of fact, and looks like that :

**Ciphertext :**

nczwvuxpnyminhzxmqsfxwlkjahshnmcoccakuqpmkcsmh  
kseinjus

blkiosxckubhmllxcsjusrrdvkohulxwccbgvliyxeoahxrhkkfvdre  
wezlx

obafgyujqukgrtvukameurbveksuhhvoyhabcjwmaklfklmyfvnri  
zr

vvrtkofdanjmolbgffleoprgrtflvrhowopbekvwmuqfmpwparmfh  
a

gkxiibg

### **Deciphered and in plain text :**

*From Looks:Radio signal 1132/19 contents:Forced to  
submerge during attack, depth charges. Last enemy loca-*

*tion08:30h, Marqu AJ 9863, 220 degrees, 8 nautical miles, (I  
am) following(the enemy). (Barometer) falls (by) 14*

*Millibar, NNO 4, visibility 10.*

You no longer need the NSA to assist in here, still they sure  
have contributed a lot while "[10]Eavesdropping

on Hell", didn't they?

193

[11]Distributed Computing is a powerful way to solve  
complex tasks, or at least put the PC power of the masses in  
use. It's no longer required to hire processing power on  
demand from any of these [12]jewels, but download a

client, start participating, or find a way to motivate your  
future participants. In my previous post "[13]The current

state of IP spoofing" I commented on the ANA Spoofer Project and featured a great deal of other distributed projects.

Meanwhile, the [14]StartdustAThome project also started gaining grounds, so is it [15]ETs, [16]Space dust, [17]global

IP spoofing susceptibility, or [18]unbroken Nazi's ciphers - you have the choice where to participate!

Technorati tags :

[19]Security, [20]Cryptography, [21]Enigma, [22]Distributed

1. [http://photos1.blogger.com/blogger/1933/1779/1600/novae\\_nigmadiagram.gif](http://photos1.blogger.com/blogger/1933/1779/1600/novae_nigmadiagram.gif)
2. [http://www.bytereef.org.nyud.net:8080/m4\\_project.html](http://www.bytereef.org.nyud.net:8080/m4_project.html)
3. <http://members.fortunecity.com/jpeschel/erskin.htm>
4. <http://www.bytereef.org.nyud.net:8080/howto/m4-project/enigma-client-unix-install.html>
5. <http://www.bytereef.org.nyud.net:8080/howto/m4-project/enigma-client-win98-install.html>
6. <http://www.bytereef.org.nyud.net:8080/howto/m4-project/enigma-client-win2000-install.html>
7. <http://www.bytereef.org.nyud.net:8080/howto/m4-project/enigma-client-winXP-Home-install.html>
8. <http://www.bytereef.org.nyud.net:8080/howto/m4-project/enigma-client-winXP-Pro-install.html>

9. <http://www.bytereef.org.nyud.net:8080/m4-project-first-break.html>
10. <http://www.nsa.gov/publications/publi00043.pdf>
11. [http://en.wikipedia.org/wiki/Distributed\\_computing](http://en.wikipedia.org/wiki/Distributed_computing)
12. <http://www.top500.org/lists/2005/11/basic>
13. <http://ddanchev.blogspot.com/2006/02/current-state-of-ip-spoofing.html>
14. <http://stardustathome.ssl.berkeley.edu/>
15. <http://setiathome.berkeley.edu/>
16. <http://stardustathome.ssl.berkeley.edu/>
17. <http://spoofer.csail.mit.edu/>
18. <http://www.hut-six.co.uk/ebreaker/index.html>
19. <http://technorati.com/tag/Security>
20. <http://technorati.com/tag/Cryptography>
21. <http://technorati.com/tag/Enigma>
22. <http://technorati.com/tag/Distributed>

194

## **2.3**

### **March**

195

**DVD of the (past) weekend (2006-03-06 14:12)**

Hi folks, as I've been down for a couple of days, I'm actively updating my blog, so watch out for some quality posts

later on and apologies for the downtime. Thanks for the interest and the questions received whatsoever!

So, after the "[1]Lone Gunmen", and "[2]The Outer Limits - Sex And Science Fiction Collection" it was about time we go beyond cyberspace with the second part of the "[3]Lawnmower man" a classic [4]techno thriller, with a lot of VR, Cyberpunks, and futuristic scenarios.

Favo [5]quote from part one - *"I find a way out, or I die in this diseased main frame"* which is also worth watching as a matter of fact. I'm so excited of seeing [6]Ray Kurzweil's views of the future in a DVD box. I am

especially interested into [7]Cyberware, and the biological adaptation with technologies. As a matter of fact, there

have already been reported cases of people with [8]implanted RFID chips, and while they wish they had [9]Johnny

Mnemonic's view of the Internet, that must be some kind of a joke. Picture yourself scanned and monitored

wherever you go while walking around with a false sense of security. RFID is a lot of buzz, I feel the potential for

information sharing, and resources cutting is outstanding, still, the levels of security or lack of understanding on the privacy implications is the biggest downside so far.

Would we someday build an [10]AI that would crawl the Universe forever colonizing the obeying the morale



we learnt "it" to? I find this such a great idea :)

Some resources on Cyberware and Cyberpunks :

[11]The Cyberpunk Project

[12]Cyberpunk

[13]"Cyberpunks in Cyberspace"

[14]Cyberanarchists, Neuromantics and Virtual Morality

[15]Cyberpunks and their online activities

[16]Cyberpunk - Ebook

[17]Cyberware Technology

[18]Realistic and Affordable Cyberware Opponents for the Information Warfare BattleSpace

[19]Cyberware Implants

196

Technorati tags :

[20]Lone Gunmen, [21]The Outer Limits, [22]Lawnmower Man, [23]Ray Kurzweil, [24]Cyberware, [25]Cyberpunk

1. <http://ddanchev.blogspot.com/2006/02/dvd-of-weekend-lone-gunmen.html>

2. <http://ddanchev.blogspot.com/2006/02/dvd-of-weekend-outer-limits-sex-and.html>

3. <http://www.amazon.com/gp/product/B0000AZT7B/103-5082892-6451063?v=glance&n=130>

4. <http://en.wikipedia.org/wiki/Techno-thriller>
5. [http://www.script-o-rama.com/movie\\_scripts/l/lawnmower-man-script-transcript-king.html](http://www.script-o-rama.com/movie_scripts/l/lawnmower-man-script-transcript-king.html)
6. <http://media.kurzweilai.net/kain/pub/RayKurzweilReader.pdf>
7. <http://en.wikipedia.org/wiki/Cyberware>
8. [http://seattletimes.nwsources.com/html/localnews/2002835871\\_chipimplant01.html](http://seattletimes.nwsources.com/html/localnews/2002835871_chipimplant01.html)
9. <http://www.cybergeography.org/atlas/johnny.jpg>
10. <http://www.imdb.com/title/tt0083658/>
11. <http://project.cyberpunk.ru/>
12. <http://en.wikipedia.org/wiki/Cyberpunk>
13. <http://www.si.umich.edu/~pne/cyberpunks.htm>
14. <http://www.dvara.net/HK/THESIS.PDF>
15. <http://www-users.rwth-aachen.de/markus.wiemker/pdf/cyberpunk.pdf>
16. <http://www.spedro.com/cyb3rpnk.pdf>
17. [http://www.cyberpunks.org/freeside/mab\\_cyber.html](http://www.cyberpunks.org/freeside/mab_cyber.html)
18. [http://www.dodccrp.org/events/2003/8th\\_ICCRTS/pdf/123.pdf](http://www.dodccrp.org/events/2003/8th_ICCRTS/pdf/123.pdf)
19. <http://www.lumrix.net/medical/implants/cyberware.html>

20. <http://technorati.com/tag/Lone+Gunmen>
21. <http://technorati.com/tag/The+Outher+Limits>
22. <http://technorati.com/tag/Lawnmower+Man>
23. <http://technorati.com/tag/Ray+Kurzweil>
24. <http://technorati.com/tag/Cyberware>
25. <http://technorati.com/tag/Cyberpunk>

197

## **February's Security Streams (2006-03-06 14:44)**

[1]It's about time I summarize all my February's Security Streams, you can of course go through my [2]January's

Security Streams as well, in case you're interested in what was inspiring me to blog during January. The truth is - **you**, the 4,477 unique and 580 unique visitors returning during the entire February, and as this blog is melting down due

to its audience and content, thanks for your time! As a matter of fact, it's been a while since I've last participated in students' thesis, but who knows these days :)

**1.** "[3]Suri Pluma - a satellite image processing tool and visualizer", treat tool I recommended to everyone interested in that type of tools, as a matter of fact, I also got many other suggestions for alternatives. More on

[4]visualization

**2.** "[5]CME - 24 aka Nyxem, and who's infected?" a small update on the Nyxem threat if any during Febru-

ary

**3.** "[6]What search engines know, or may find out about us?" a commentary on a CNET's Q &A with leading search engines on how they deal with subpoenas and user's privacy, further resources and opinions on the topic are

provided as well. Anything that can be linked will be one way or another.

**4.**

"[7]The current state of IP spoofing" introducing the ANA Spoofer Project, commentary on the current

state according to their sample, and many other distributed concepts again related to security are mentioned

**5.** "[8]Hacktivism tensions" A brief coverage of the mass defacements of Danish sites out of the Muhamad's cartoons distribution over Europe, and of course, over the Net. I also mentioned a previous rather more severe case

or Nation2Nation cyberwarfare PSYOPS attacks

**6.** "[9]Security Awareness Posters" a small list with links to free security awareness posters worth using or enjoying their witty messages

**7.** "[10]A top level espionage case in Greece" With the great possibility of an insider's job, the eavesdropping of major government officials and citizens was indeed the second case that made me an impression, next to the

stone transmitter found in a Moscow's park

**8.** "[11]The War against botnets and DDoS attacks" A post covering the introduction of McAfee's bot killing system, The ZombieAlert Service, some comments and lots of external resources on fighting and protecting against

Botnets and DDoS attacks

198

**9.** "[12]Who needs nuclear weapons anymore?" An in-depth article I wrote while coming across a news article on a recent EMP warhead test, with the idea to bring more awareness on the potential of EMP weapons, some of

the current trends, and the emerging weaponization of Space . A [13]reader also mentioned a [14]Mig-25 [15]found

on Google Maps

**10.** "[16]Recent Malware developments" a post summarizing various events right in the middle of February, discussing some of the emerging trends to keep an eye on, a commentary on Kaspersky's summary for 2005, worth

checking out as well

**11.** "[17]Look who's gonna cash for evaluating the maliciousness of the Web?" Crawling for malware and evaluating the maliciousness of the Web with automated patrol for sites distribution it is a very hot and feasible topic

you can learn more about by reading this post

**12.** "[18]Detecting intruders and where to look for" comments and external resources related to rootkits and forensics

**13.** "[19]A timeframe on the purchased/sold WMF vulnerability" as requested by readers

**14.** "[20]The end of passwords - for sure, but when?" As my first blog post was related to passwords security and why bother given their major insecurities, in this post I commented Bill Gate's remarks. I think they don't know

what they are really up to at the bottom line

**15.** "[21]Smoking emails" Would you pay millions to avoid paying billions and keep a clean image? Of course you will!

**16.** "[22]DVD of the weekend - The Lone Gunmen" the first post related to DVDs worth watching over the

weekend

**17.** "[23]How to win 10,000 bucks until the end of March?" Find a critical, as defined by Microsoft's security bulletins, vulnerability, participate in the [24]market for software vulnerabilities - the future Obay, and sell it to

iDefense for 10,000 bucks, but what about the social outcome out of the process, if any?

199

**18.** "[25]Chinese Internet Censorship efforts and the outbreak" recent events related to the Chinese efforts to monitor and censor the web, the the "West's" reactions. I did quite a lot of quality posts on the topic during January and February mainly because I feel that the higher the publicity for the problem, the higher the pressure towards

starting talks on the future of these efforts

**19.** "[26]Master of the Infected Puppets" comments on botnets communication provoked out of a nice [27]research I came across to

**20.** "[28]Give it back!" Mixed signals from the CIA, DIA and the DoJ on secrecy

**21.** "[29]One bite only, at least so far!" a brief coverage of the OS X trojan and the InqTana worm

**22.** "[30]DVD of the Weekend - The Outer Limits - Sex And Science Fiction Collection" weekend two, second DVD

**23.** "[31]Get the chance to crack unbroken Nazi Enigma ciphers" another distributed concept this time cracking unbroken Nazi messages

Technorati tags :

[32]Security, [33]Information Security

1.

[http://photos1.blogger.com/blogger/1933/1779/1600/Mind%20blowing\\_Nicholas%20Cann.1.jpg](http://photos1.blogger.com/blogger/1933/1779/1600/Mind%20blowing_Nicholas%20Cann.1.jpg)

2. <http://ddanchev.blogspot.com/2006/01/januarys-security-streams.html>

3. <http://ddanchev.blogspot.com/2006/02/suri-pluma-satellite-image-processing.html>

4. <http://ddanchev.blogspot.com/2006/01/visualization-intelligence-and.html>

5. <http://ddanchev.blogspot.com/2006/02/cme-24-aka-nyxem-and-whos-infected.html>

6. <http://ddanchev.blogspot.com/2006/02/what-search-engines-know-or-may-find.html>
7. <http://ddanchev.blogspot.com/2006/02/current-state-of-ip-spoofing.html>
8. <http://ddanchev.blogspot.com/2006/02/hackivism-tensions.html>
9. <http://ddanchev.blogspot.com/2006/02/security-awareness-posters.html>
10. <http://ddanchev.blogspot.com/2006/02/top-level-espionage-case-in-greece.html>
11. <http://ddanchev.blogspot.com/2006/02/war-against-botnets-and-ddos-attacks.html>
12. <http://ddanchev.blogspot.com/2006/02/who-needs-nuclear-weapons-anymore.html>
13. <http://www.blogger.com/comment.g?blogID=18493443&postID=113951123538868270>
14. [http://en.wikipedia.org/wiki/Mig\\_25](http://en.wikipedia.org/wiki/Mig_25)

200

15. <http://maps.google.com/maps?q=Albuquerque,+NM&t=k&amp;amp;amp;hl=en&ll=35.048845,-106.575813&spn=0.001043,0.002682&t=k>
16. <http://ddanchev.blogspot.com/2006/02/recent-malware-developments.html>



17. <http://ddanchev.blogspot.com/2006/02/look-whos-gonna-cash-for-evaluating.html>
18. <http://ddanchev.blogspot.com/2006/02/detecting-intruders-and-where-to-look.html>
19. <http://ddanchev.blogspot.com/2006/02/timeframe-on-purchasedsold-wmf.html>
20. <http://ddanchev.blogspot.com/2006/02/end-of-passwords-for-sure-but-when.html>
21. <http://ddanchev.blogspot.com/2006/02/smoking-emails.html>
22. <http://ddanchev.blogspot.com/2006/02/dvd-of-weekend-lone-gunmen.html>
23. <http://ddanchev.blogspot.com/2006/02/how-to-win-10000-bucks-until-end-of.html>
24. <http://ddanchev.blogspot.com/2005/12/0bay-how-realistic-is-market-for.html>
25. <http://ddanchev.blogspot.com/2006/02/chinese-internet-censorship-efforts.html>
26. <http://ddanchev.blogspot.com/2006/02/master-of-infected-puppets.html>
27. [http://www.cs.wisc.edu/~pb/botnets\\_final.pdf](http://www.cs.wisc.edu/~pb/botnets_final.pdf)
28. <http://ddanchev.blogspot.com/2006/02/give-it-back.html>
29. <http://ddanchev.blogspot.com/2006/02/one-bite-only-at-least-so-far.html>

30. <http://ddanchev.blogspot.com/2006/02/dvd-of-weekend-outer-limits-sex-and.html>

31. <http://ddanchev.blogspot.com/2006/02/get-chance-to-crack-unbroken-nazi.html>

32. <http://technorati.com/tag/Security>

33. <http://technorati.com/tag/Information+Security>

201

### **Anti Phishing toolbars - can you trust them? (2006-03-06 16:04)**

A lot of recent [1]phishing events occurred, and what should be mentioned is their constant ambitions towards

increasing the number of trust points between end users and the mirror version of the original site. The use of SSL

and the ease of obtaining a valid certificate for to-be fraudulent domain is a fairly simple practice. Phishing is so much more than this, and it even has to do with [2]buying 0day [3]vulnerabilities to keep itself competitive.

How should phishing be fought? Educating the end user not to trust that he/she's on Amazon.com, when he

just typed it, or enforcing a technological solution to the problem of digital social engineering and trust building? As far as trends are concerned, according to the [4]AntiPhishingGroup's latest report :

- *Number of unique phishing reports received in December: 15244*

- *Number of unique phishing sites received in December: 7197*
- *Number of brands hijacked by phishing campaigns in December: 121*
- *Number of brands comprising the top 80 % of phishing campaigns in December: 7*
- *Country hosting the most phishing websites in December: United States*
- *Contain some form of target name in URL: 51 %*
- *No hostname just IP address: 32 %*
- *Percentage of sites not using port 80: 7 %*
- *Average time online for site: 5.3 days*
- *Longest time online for site: 31 days*

*In case you haven't come across to this research "[5]Do Security Toolbars Actually Prevent Phishing Attacks?"*

*you'll find that it has very good points and actual evidence. Antiphishing filters and toolbars protection are gaining popularity, and many popular companies are fighting for market share of the end users'*

desktop, but keep in mind that :

*"We conducted two user studies of three security toolbars and other browser security indicators and found*

*them all ineffective at preventing phishing attacks. Even though subjects were asked to pay attention to the toolbar,*

*many failed to look at it; others disregarded or explained away the toolbars' warnings if the content of web pages*

*looked legitimate. We found that many subjects do not understand phishing attacks or realize how sophisticated such*

*attacks can be."*

The topic of phishing and fighting the problem has been again greatly extended by the researcher [6]Min Xu,

while writing the thesis "[7]Fighting Phishing at the User Interface" and introducing a solution that measures a site's reputation and trustfulness. While, this is among the simplest ways Google uses to while assigning PageRank's, I find

this a common sense warning. Still, with the constant flood of Web 2.0 companies, does it matter? :) Check out

some screenshots from this outstanding thesis, and get the point :

202

Localizing the attacks, taking advantage of the momentum, or a software vulnerability within a popular browser or site itself, as well as taking advantage of malware, are among the most common practices these days. Moreover, I

feel that fighting phishing the wrong way could [8]erode the end user's trust in the Web on the other hand, so do

your homework on the social impact on anything you do. [9]NetCraft's Anti Phishing toolbar, whatsoever, is my

favorite combination of them all, still, awareness and lack of naivety when it comes to transactions or authentication

is the perfect tool, what about yours?

Some resources worth mentioning are :

[10]Candid's [11]"Phishing in the middle of the stream"  
Today's threats to online banking

[12]Know your Enemy : Phishing

[13]Phishing attacks and countermeasures

[14]The Phishing Guide

[15]Distributed Phishing Attacks

[16]Phishiest Countries

[17]MailFrontier Phishing IQ Test

[18]Online Identity Theft: Phishing Technology, Chokepoints and Countermeasures

Technorati tags :

[19]Security, [20]Phishing, [21]Toolbar, [22]AntiPhishing Group

1. <http://isc.sans.org/diary.php?storyid=1118>

2. <http://ddanchev.blogspot.com/2006/01/was-wmf-vulnerability-purchased-for.html>

3. <http://ddanchev.blogspot.com/2005/12/0bay-how-realistic-is-market-for.html>

4. [http://www.antiphishing.org/reports/apwg\\_report\\_DEC2005\\_FINAL.pdf](http://www.antiphishing.org/reports/apwg_report_DEC2005_FINAL.pdf)
5. <http://groups.csail.mit.edu/uid/projects/phishing/chi-security-toolbar.pdf>
6. <http://www.ece.umd.edu/~minwu/>
7. <http://groups.csail.mit.edu/uid/projects/phishing/proposal.pdf>
8. <http://ddanchev.blogspot.com/2006/01/hidden-internet-economy.html>
9. <http://toolbar.netcraft.com/>
10. <http://www.wueest.ch/dublin/>
11. [http://www.trojan.ch/paper/ThreatsToOnlineBanking\\_Candid\\_Wueest.pdf](http://www.trojan.ch/paper/ThreatsToOnlineBanking_Candid_Wueest.pdf)
12. <http://www.honeynet.org/papers/phishing/>
13. <http://www.cert-in.org.in/knowledgebase/whitepapers/ciwp-2005-03.pdf>
14. <http://www.ngssoftware.com/papers/NISR-WP-Phishing.pdf>
15. <http://eprint.iacr.org/2005/091.pdf>
16. <http://toolbar.netcraft.com/stats/countries>
17. <http://survey.mailfrontier.com/survey/quiztest.html>

18. <http://www.antiphishing.org/Phishing-dhs-report.pdf>
19. <http://technorati.com/tag/Security>
20. <http://technorati.com/tag/Phishing>
21. <http://technorati.com/tag/Toolbar>
22. <http://technorati.com/tag/AntiPhishing+Group>

203

### **Data mining, terrorism and security (2006-03-06 19:53)**

[1]I've been actively building awareness on what used to feel like an unpopular belief only - [2]Cyberterrorism, and also covered some [3]recent events related to Cyberterrorism in some of my previous posts.

Last week, The NYTimes wrote about "[4]Taking Spying to Higher Level, Agencies Look for More Ways to Mine

Data", and I feel that avoiding the mainstream media for the sake of keeping it objective is quite useful sometimes.

From the article :

*"On the wish list, according to several venture capitalists who met with the officials, were an array of tech-*

*nologies that underlie the fierce debate over the Bush administration's anti-terrorist eavesdropping program:*

*computerized systems that reveal connections between seemingly innocuous and unrelated pieces of information.*

*The tools they were looking for are new, but their application would fall under the well-established practice of data mining: using mathematical and statistical techniques to scan for hidden relationships in streams of digital data or large databases."*

Interest in harnessing the power of data mining given the enormous flow of information from different par-

ties would never cease to exist. What's more to note in this case, is the [5]Able Danger scenario as a key indicator for usefulness of outdated information, given any has been there at the first place. Conspiracy theorists would logically

conclude that the need for evidence of the power of data mining for tracking terrorists would inevitably fuel more

investments in this area. So true, and here's a recent event to keep the discussing going - "[6]Suit airs Able Danger claims: Two operatives in secret program say their lawyers were barred at hearings"

While on one hand wars are getting waged with the idea to eradicate terrorist deep from its roots, and sort of

building "local presence" thus improving assets allocation and intelligence gathering, I feel the fact that a reliable communication channel could be established by a terrorist network over the Net is already gaining a lot of necessary

attention. However, TIA's ambitions have always been desperately megalomaniac, what about some marginal

thinking in here folks, you cannot absorb all the info and make sense out of it, and who says it has to be all of it at the first place?!



[7]The Total Information Awareness program was prone to be abused in one way or another, like pretty much

any data mining system from my point of view. And while it's supposidely down due to budget deficits and privacy

violations outbreak, government legislation and ensuring [8]key networks remain wiretaps-ready seems to be a

valuable asset for any future data mining projects. [9]TIA is still up and running folks, or even if it's not using the

same name, the concept is still in between the lines of [10]DHS's budget for 2006 and would always be, and with the

majority of corporate sector's participants are [11]opening up their networks to comply with "legal requirements", the lines between privacy and the war against terrorism, and what to exchange for what, seems to be getting even

more shady these days.

204

In my previous posts, I also mentioned about the power of the [12]Starlight project as existing initiative to data mine data from different and media-rich sources alltogether, and most importantly, visualize the output. If you

fear BigBrother, don't fear the Eye, but fear the Eyeglasses :)

More resources on Data Mining and Terrorism :

[13]Data Mining : An Overview

[14]Data Mining and Homeland Security : An Overview  
(updated January 27, 2006)

[15]Using data mining techniques for detecting terror-  
related web activities

[16]Data mining and surveillance in the post-9.11  
environment

[17]The Dark Web Portal: Collecting and Analyzing the  
Presence of Domestic and International Terrorist Groups on  
the Web

[18]Workshop on Data Mining for Counter Terrorism and  
Security

[19]TRAKS: Terrorist Related Assessment using Knowledge  
Similarity

[20]The Multi-State Anti-Terrorism Information Exchange  
(MATRIX)

[21]A Knowledge Discovery Approach to Addressing the  
Threats of Terrorism - [22]w00t

[23]Gyre's Data Mining section

[24]Eyeballing Total Information Awareness

[25]Able Danger blog

[26]EPIC's TIA section

[27]EFF's TIA section

Technorati tags : [28]Security, [29]Terrorism,  
[30]Cyberterrorism, [31]Data Mining, [32]TIA

1. [http://photos1.blogger.com/blogger/1933/1779/1600/total\\_information\\_awareness.1.png](http://photos1.blogger.com/blogger/1933/1779/1600/total_information_awareness.1.png)
2. <http://ddanchev.blogspot.com/2005/12/cyberterrorism-dont-stereotype-and-its.html>
3. <http://ddanchev.blogspot.com/2006/01/cyberterrorism-recent-developments.html>
4. <http://www.nytimes.com/2006/02/25/technology/25data.html>
5. [http://en.wikipedia.org/wiki/Able\\_Danger](http://en.wikipedia.org/wiki/Able_Danger)
6. <http://www.tmcnet.com/usubmit/2006/03/04/1428870.htm>
7. [http://en.wikipedia.org/wiki/Information\\_Awareness\\_Office](http://en.wikipedia.org/wiki/Information_Awareness_Office)
8. <http://www.blackhat.com/presentations/bh-usa-03/bh-us-03-baloo.pdf>
9. <http://nationaljournal.com/about/njweekly/stories/2006/0223nj1.htm>
10. [http://www.dhs.gov/dhspublic/interapp/press\\_release/press\\_release\\_0613.xml](http://www.dhs.gov/dhspublic/interapp/press_release/press_release_0613.xml)
11. <http://www.cdt.org/publications/200408dempseyflint.pdf>
12. <http://ddanchev.blogspot.com/2006/01/visualization-intelligence-and.html>

13. <http://www.fas.org/irp/crs/RL31798.pdf>
14. <http://www.fas.org/sgp/crs/intel/RL31798.pdf>
15. [http://www.ise.bgu.ac.il/faculty/mlast/papers/JIW\\_Paper.pdf](http://www.ise.bgu.ac.il/faculty/mlast/papers/JIW_Paper.pdf)
16. <http://www.asc.upenn.edu/usr/ogandy/IAMCRdatamining.pdf>
17. [http://ai.bpa.arizona.edu/research/terror/publications/ITCS\\_Dark\\_Web\\_submission.pdf](http://ai.bpa.arizona.edu/research/terror/publications/ITCS_Dark_Web_submission.pdf)
18. <http://ic.arc.nasa.gov/publications/pdf/Data%20Mining%20for%20Counter%20Terrorism%20SIAM%202003%20Workshop%20Proceedings.pdf>
19. [http://lsdis.cs.uga.edu/proj/traks/about/final\\_report.pdf](http://lsdis.cs.uga.edu/proj/traks/about/final_report.pdf)
20. <http://www.fas.org/irp/crs/RL32536.pdf>
- 205
21. [http://ai.bpa.arizona.edu/people/edna/AILab\\_terrorism%20Knowledge%20Discovery%20ISI%20\\_apr04.pdf](http://ai.bpa.arizona.edu/people/edna/AILab_terrorism%20Knowledge%20Discovery%20ISI%20_apr04.pdf)
22. [http://ai.bpa.arizona.edu/paper\\_conf/index.htm](http://ai.bpa.arizona.edu/paper_conf/index.htm)
23. <http://www.gyre.org/news/related/Data+Mining>
24. <http://eyeball-series.org/tia-eyeball.htm>
25. <http://www.abledangerblog.com/>

26. <http://www.epic.org/privacy/profiling/tia/>

27. <http://www.eff.org/Privacy/TIA/>

28. <http://technorati.com/tag/Security>

29. <http://technorati.com/tag/Terrorism>

30. <http://technorati.com/tag/Cyberterrorism>

31. <http://technorati.com/tag/Data+Mining>

32. <http://technorati.com/tag/TIA>

206

### **5 things Microsoft can do to secure the Internet, and why it wouldn't? (2006-03-06 20:21)**

[1]In my previous post on Internet security, I was just scratching the surface of "[2]How to secure the Internet", and emphasized that plain text communications, insecure by design, and our [3]inability to measure the costs of cybercrime, are among the things to keep in mind.

Now, If I were asked about [4]monocultures, "ship it now, patch it later" attitudes or slow reactive approaches, I would quickly ask is it Microsoft you're talking about? It's a common weakness to blame the most popular or richest

companies before rethinking the situation, or even worse, waiting for someone else to secure you, instead of you

trying to figure out how to achieve the balance. Is [5]Linux, [6]or, [7]OS X more secure than Microsoft's Windows, or

they are just not popular enough to achieve the scale of vulnerabilities, even interest in exploiting their weaknesses?

Important questions arise as always :

- Are Microsoft's products insecure by default, or what is insecure in this case?

- Should Microsoft's number of known vulnerabilities act as a benchmark for commitment towards security, quality

of the software, or should this be totally excluded given the tempting target Microsoft's products really are?

- Should a vendor be held liable for not releasing a patch in a timely fashion, and what are the acceptable timeframes,

given how quickly malware authors take advantage, and "worm the vulnerability"?

These and many other points led me to the idea of brainstorming on what Microsoft could do to secure the

Internet as a whole, and contribute to the social welfare of the society(a [8] \$100 laptop powered by a hand crank,

is so much better than a [9]smartphone, given it's education, and not entertainment you're looking for! ). This is

not an anti-microsoft oriented post, they've got enough [10]anti-trust legislations and Vista issues to deal with, yet,

it's a summary of my thoughts while going through Slashdot's chat with [11]Mike Nash VP of security, and some

Microsoft's [12]comments on today's state of the [13]market for software vulnerabilities.

## 1. Think twice before reinventing the security industry

What is the first thing that comes across your mind when you picture Microsoft as a security vendor? A worst

case scenario for the Internet as a whole? Just kidding, but still, with such a powerful brand, BETA products, and their legal monopoly from my point of view, is quite a good foundation besides [14]constant [15]acquisitions. Microsoft

is a software company, software innovation is among their core competencies. Yet, today's fast growing information

security market opens up many more profitable opportunities. Though, I'd rather they stick to their current OEM

licensing agreements by the time they actually come up with something truly unique. Acquiring companies indeed

improves competitiveness, but is it just me seeing the irony of entering the security industry without first dealing

with the idea internally? The introduction of a [16]OS build-in firewall, and bi-directional and fully working with IPSec for Vista would immediately provide Microsoft with a great opportunity to start serving certain market segments,

while it would leave them in experimental mode while MS is gaining the experience.

207

### **Why it wouldn't?**

Because the information security market is growing so steadily, that if Microsoft doesn't take a piece of the

pie, it would be a totally flawed business logic. And they want to do it as independently, thus more profitably, as

possible. The recent [17]FBI's 2005 Computer Crime Survey indicated that the majority of security dollars are spent

on antivirus, antispyware, and perimeter based security solutions, no one would miss that opportunity. While you

can acquire competitive advantage, and actually buy yourself an anti virus vendor, you cannot do the same with core

competencies, moreover, I once said "less branding, but higher preferences", and you might end up making the right decision for the time being. Moreover, to operate in today's anti virus market you need a brand name and if you don't

have it, there's a great chance you wouldn't be able to gain any market share, of course if you you don't somehow

capitalize on a niche, and introduce innovative competitive features. The rest is all about OEM agreements and

licensing technologies or the opportunity to provide a service, still, it's Microsoft's brand and market development

practices to worry about. [18]Passport, [19]Trustworthy Computing, [20]InfoCard it's all under Microsoft's Brand

umbrella.

**2.** Become accountable, first, in front of itself, than, in front of the its stakeholders

What is accountability in this case anyway? Releasing a patch given a vulnerability is known within a prede-



fined timeframe? Set, report and improve its own benchmark on a fast response towards a security threat?  
Overall

commitment as a whole? You cannot simply say “hold on” when the entire world is waiting for you to release a patch,

any excuse in such a situation should be considered as lack of responsibility. And given that no vendor has been

held liable for not releasing a patch in a timely manner, why would they bother to be the benchmark? I think the

problem isn't the lack of resources, but understanding the importance of it. Microsoft is so huge and powerful that's

its clumsiness is in direct proportion with this fact, isn't it. Can [21]Elephants Indeed Dance in this case? Microsoft's VP of Security [22]Mike Nash, made a lot of comments for a [23]Slashdot interview that made me an impression,

such as :

*“Four years ago, I used to have to have frequent conversations with teams who would tell me that they couldn't go*

*through the security review process because they had competitive pressures or had made a commitment to partners*

*to ship at a certain time.”* – I can argue that nothing has changed since then, can you?

**Why it wouldn't?**

Mainly because of the actual commitment, though I feel Microsoft could evolve if it manages to find the bal-

ance between being a software company with ambitions in the security industry. First, the clear benefits should be

understood, and they obviously aren't. I greatly feel that until a customer, or a legal party doesn't start questioning

various practices, this self-regulation is not getting us anywhere. Gratefully, there are independent researchers out

there that have a point way faster than the vendor itself. I think exchanging information in a way that satisfies

both parties would be the best thing to do. Employees training without successful evaluation of the progress is

useless, and while seeking accountability from a programmer has been greatly discussed, I feel that outsourcing the

auditing is always an option worth keeping in mind. Would confidentiality of the ultra-secret Microsoft's code be

breached? I doubt so given they implement close activities monitoring and the Manhattan project style operations

208

and cooperation between teams.

Don't get me wrong, Microsoft's software will always be blamed for being insecure, but instead I feel its de-

facto position as an OS turns it into an exciting daily research topic, whereas its anti-trust compliance practices

such as sharing technical details so that competitors could – puts them in a very unfavourable \$279.83B [24]market

capitalization position. Security shouldn't be something to live with as if it's normal, instead it should be provoked

by means of active testing and proactive solutions. I feel what they are missing is a legal incentive to promptly

comply with patch releases, while on the other hand can you picture the outcome of a minor tax deduction in case a

milestone in the release of proactive security vulnerabilities is reached, and watch them securing!

**3.** Reach the proactive level, and avoid the reactive, in respect to software vulnerabilities

Have you even imagined Microsoft releasing proactive patches to fix 0day vulnerabilities it has managed to

find out through third-party code auditing practices, or within its internal quality assurance departments? Sounds too

good to be true, but reaching the proactive level is an important step, so hold your breath, they did it with [25]Vista

already! Still, their practices with dealing with the reactive response are questionable, and as it often happens, the

window of opportunity due to their efforts to testing and localizing the patches for all their customers(the entire

world) is causing windows of opportunities that I could argue drive the security industry.

**Why it wouldn't?**

Resources and commitment, though the first can be successfully outsourced. What I greatly feel the company is missing is a clear strategy towards understanding the benefits, and eventually the commitment to do it. Microsoft isn't insanely obsessed with the idea to provide bugs free software, but features rich one. And the way MSN is not going to get more allocated budget compared to MS Office, it's going to take a while by the time they realize the importance and key role they play as being on the majority of PC and servers worldwide. Some [26]comments again :

*"I often get asked the question, "who has been fired for shipping insecure code at Microsoft?" My usual answer here is that we are still learning a lot about security at Microsoft and that most of the security issues that we deal with don't come as a result of carelessness or disregard for the process, but rather new vectors of attack that we didn't understand at the time."*

**4.** Introduce an internal security oriented culture, or better utilize its workforce in respect to security

[27]Google's 70/20/10 rule is an example, and while Microsoft tends to position itself as THE software com-

pany, to some it may be competing with other major software vendors, or the Open Source threat, it actually

competes on [28]IQ basis. Flame them, talk whatever you want, they are still able to attract the smartest people

on Earth to work for them. My point is, that introducing a Google style culture, where engineers and anyone from

their employees spend 10 % of their time on personal projects, this time towards security, it would inevitable make

an impact on finding the balance between usability and security on any of its products. Devoting any percentage of

209

work time towards security related projects and initiatives would.

### **Why it wouldn't?**

They pretend they have their own corporate citizenship methods, and moreover, [29]they hate Google with a

reason. Or is it about the culture, spending time on security/hacking cons to find out that's driving the industry, or

basically stop shipping products with the majority of features turned on by default with the idea to "show off" their features?

### **5. Rethink its position in the security vulnerabilities market**

Would this mean there would be more monopolistic sentiments?

I'm just kiddin' of course though it's still

questionable. Would a Microsoft's initiative to recruit outstanding vulnerability researchers and actually purchase

their research have any effect at all? It would definitely help them I cannot actually imagine Microsoft paying for

Oday IE vulnerabilities, but I can literally see them catching up with week delay on the WMF vulnerability. But the

usefulness and the potential of this approach are enormous, and the intelligence gathered will provide them with

unique business development opportunities, given they actually take advantage of them.

Microsoft has stated numerous time that it doesn't agree with the practice of buying security vulnerabilities,

and while I also don't agree that commercializing the current state of the process of discovering, exploiting, and

patching is the smartest thing to do, picture a \$250k bounty for information leading to the arrest of virus writers

being spent on secure code auditing, or push/pull software vulnerabilities approach with reputable researchers only

- it would make a change for sure.

### **Why it wouldn't?**

Because the biggest problem of a 800 pound gorilla is its EGO with capital letters. We are not interested in

pulling intelligence from you, we are interested in pushing you the final results branded with Microsoft's logo. Is it

profitable? It is. Is it realistic in today's collective intelligence dominated Web? It isn't, and the whole concept has to go beyond Live.com from my point of view. Until, then, let's still say a big thanks for playing such a vital role in our society's progress, but no one seems to tolerate the security trade-offs anymore, that's a fact.

To conclude, as I've said I think it isn't the lack of resources, but understanding the importance of the issue.

What do you think, what else can Microsoft do, and why it wouldn't? :)

Technorati tags :

210

[30]Security, [31]Microsoft

1. [http://photos1.blogger.com/blogger/1933/1779/1600/Microsoft\\_vs\\_Linux.0.jpg](http://photos1.blogger.com/blogger/1933/1779/1600/Microsoft_vs_Linux.0.jpg)
2. <http://ddanchev.blogspot.com/2006/01/how-to-secure-internet.html>
3. <http://ddanchev.blogspot.com/2006/01/why-we-cannot-measure-real-cost-of.html>
4. <http://www.ccianet.org/papers/cyberinsecurity.pdf>
5. <http://download.microsoft.com/download/1/e/e/1ee952f2-2287-4cc3-8ccd-03bb62e38e5a/SecInnovation.pdf>
6. [http://www.theregister.co.uk/2004/10/22/security\\_report\\_windows\\_vs\\_linux.pdf](http://www.theregister.co.uk/2004/10/22/security_report_windows_vs_linux.pdf)
7. [http://images.apple.com/macosx/pdf/Mac\\_OS\\_X\\_Security\\_TB.pdf](http://images.apple.com/macosx/pdf/Mac_OS_X_Security_TB.pdf)
8. <http://laptop.media.mit.edu/>
9. <http://www.mobilemag.com/content/100/344/C6248/>

10. [http://www.theregister.co.uk/2006/02/28/microsoft\\_appeals\\_antitrust\\_ruling/](http://www.theregister.co.uk/2006/02/28/microsoft_appeals_antitrust_ruling/)
11. <http://interviews.slashdot.org/article.pl?sid=06/01/26/131246>
12. <http://www.eweek.com/article2/0,1895,1928389,00.asp>
13. <http://ddanchev.blogspot.com/2005/12/0bay-how-realistic-is-market-for.html>
14. <http://www.itsecurity.com/security.htm?s=4609&sid=706b24694ae2d0bd495fae92fba03abd>
15. <http://www.microsoft.com/presspass/press/2004/dec04/12-16GIANTPR.mspx>
16. <http://www.microsoft.com/athome/security/spyware/software/default.mspx>
17. <http://ddanchev.blogspot.com/2006/01/fbis-2005-computer-crime-survey-whats.html>
18. <http://www.passport.net/>
19. <http://www.microsoft.com/mscorp/twc/default.mspx>
20. <http://www.microsoft.com/presspass/features/2006/feb06/02-14InfoCards.mspx>
21. <http://www.amazon.com/gp/product/0060523794/102-9691797-5904134?v=glance&n=283155>



22. <http://www.microsoft.com/presspass/exec/mnash/default.mspx>
23. <http://interviews.slashdot.org/article.pl?sid=06/01/26/131246>
24. <http://finance.yahoo.com/q/bc?s=MSFT>
25. <http://www.techworld.com/security/news/index.cfm?NewsID=5165>
26. <http://interviews.slashdot.org/article.pl?sid=06/01/26/131246>
27. <http://www.epnetwork.co.za/google-chairman.asp>
28. <http://www.forbes.com/columnists/forbes/2005/1031/045.html>
29. <http://yro.slashdot.org/article.pl?sid=05/09/03/0515250&from=rss>
30. <http://technorati.com/tag/Security>
31. <http://technorati.com/tag/Microsoft>

211

### **The Future of Privacy = don't over-empower the watchers! (2006-03-07 16:45)**

[1]I blog a lot about privacy, anonymity and censorship, mainly because I feel not just concerned, but obliged to

build awareness on the big picture the way I see it. Moreover, I find these interrelated and excluding any of

these

would result in missing the big picture, at least from my point of view. Some posts I did, worth mentioning are :

"[2]Anonymity or Privacy on the Internet?", "[3]China - the biggest black spot on the Internet's map", "[4]2006 =

1984?", "[5]Still worry about your search history and BigBrother?", "[6]The Feds, Google, MSN's reaction, and how you got "bigbrothered?", "[7]Twisted Reality", "[8]Chinese Internet Censorship efforts and the outbreak", and the most recent one, "[9]Data mining, terrorism and security".

Yesterday, I read a very nice essay by Bruce Schneier "[10]The Future of Privacy" and while I feel it has been written for the general public to understand, you can still update yourself on some of the current trends he's

highlighting, mostly the digital storage of our life activities, and how possible it really is.

Some comments that made me an impression though :

*"The typical person uses 500 cell phone minutes a month; that translates to 5 gigabytes a year to save it all.*

*My iPod can store 12 times that data. A "life recorder" you can wear on your lapel that constantly records is still a few generations off: 200 gigabytes/year for audio and 700 gigabytes/year for video." - scary stuff, but so true!*

*"Today, personal information about you is not yours; it's owned by the collector." - if you were to question the practices of each and every "collector" you wouldn't be able to properly function in the 21st century.*

*"The city of Baltimore uses aerial photography to surveil every house, looking for building permit violations." -*

typical Columbian style, still applicable in here.

*"In some ways, this tidal wave of data is the pollution problem of the information age. All information pro-*

*cesses produce it. If we ignore the problem, it will stay around forever. And the only way to successfully deal with it is to pass laws regulating its generation, use and eventual disposal."*

I agree on regulation, given someone follows and it's actually implemented, still, I feel it's all about balancing

the powers of the public and the ruling parties. The more a government is empowered to invade privacy in one

way or another, the higher the risk of them abusing their power, or even worse, having their communications

infrastructure wiretap-ready for third parties.

**UPDATE** - this post recently appeared at LinuxSecurity.com - [11]The Future of Privacy = don't over-empower

the watchers!

212

Technorati tags :

[12]Privacy, [13]Anonymity, [14]Censorship

1.

[http://photos1.blogger.com/blogger/1933/1779/1600/internet\\_privacy.1.jpg](http://photos1.blogger.com/blogger/1933/1779/1600/internet_privacy.1.jpg)

2. <http://ddanchev.blogspot.com/2006/01/anonymity-or-privacy-on-internet.html>
3. <http://ddanchev.blogspot.com/2006/01/china-biggest-black-spot-on-internets.html>
4. <http://ddanchev.blogspot.com/2006/01/2006-1984.html>
5. <http://ddanchev.blogspot.com/2006/01/still-worry-about-your-search-history.html>
6. <http://ddanchev.blogspot.com/2006/01/feds-google-msns-reaction-and-how-you.html>
7. <http://ddanchev.blogspot.com/2006/01/twisted-reality.html>
8. <http://ddanchev.blogspot.com/2006/02/chinese-internet-censorship-efforts.html>

9. <http://ddanchev.blogspot.com/2006/03/data-mining-terrorism-and-security.html>
10. [http://www.schneier.com/blog/archives/2006/03/the\\_future\\_of\\_p.html](http://www.schneier.com/blog/archives/2006/03/the_future_of_p.html)
11. <http://www.linuxsecurity.com/content/view/121999/65/>
12. <http://technorati.com/tag/Privacy>
13. <http://technorati.com/tag/Anonymity>
14. <http://technorati.com/tag/Censorship>

213

### **Where's my Oday, please? (2006-03-07 21:22)**

A [1]site I was recently monitoring disappeared these days, so I feel it's about time I blog on this case. I have been

talking about the [2]emerging market for software vulnerabilities for quite some time, and it's quite a success to come

across that the concept has been happening right there in front of us. Check out the screenshots. **The International**

**Exploits Shop** I came across to looks like this :

[3]It appears to be down now, while it has simply changed its location to somewhere else. Google no longer

has it cached, and the the only info on this wisely registered .in domain, can be found at [4]Koffix Blocker's site.

A lot of people underestimate the power of the over-the-counter(OTC), market for 0day security vulnerabili-

ties. Given that there isn't any vulnerabilities auction in place that [5]would provide a researcher with multiple

proposals, and the buyers with a much greater choice or even social networking with the idea to possibly attract

skilled HR, the seller is making personal propositions with the idea to get higher exposure from the site's visitors.

Whoever is buying the exploit and whatever happens with it doesn't seem to bother the seller in this case.

As there's been already emerging competition between different [6]infomediaries that purchase vulnerabili-

ties information and pay the researchers, researchers themselves are getting more and more interested in hearing

from "multiple parties". Turning vulnerability research, and its actual findings into an IP, and offering financial incentives is tricky, and no pioneers are needed in here!

There's been a lot of active discussion among friends, and over the Net. I recently came across a great and

very recent research entitled "[7]Vulnerability markets - what is the economic value of a zero-day exploit?", by Rainer Boehme, that's worth the read. Basically, it tries to list all the market models and possible participants, such as :

## **Bug challenges**

- Bug challenges are the simplest and oldest form of vulnerability markets, where the producer offers a monetary reward for reported bugs. There are some real-world examples for bug challenges. Most widely known is Donald E. Knuth's reward of initially 1.28 USD for each bug in his TEX typesetting system, which grows exponentially with the number of years the program is in use. Other examples include the RSA factoring challenge, or the shady SDMI challenge on digital audio watermarking

## **Bug auctions**

- Bug auctions are theoretical framework for essentially the same concept as bug challenges. Andy Ozment [9] first formulated bug challenges in the terms of auction theory, in particular as a reverse Dutch auction, or an open first-price ascending auction. This allowed him to draw on a huge body of literature and thus add a number of efficiency enhancements to the original concept. However, the existence of this market type still depends on the initiative of the vendor

214

## **Vulnerability brokers**

- Vulnerability brokers are often referred to as "vulnerability sharing circles". These clubs are

*built around independent organizations (mostly private companies) who offer money for new vulnerability reports,*

*which they circulate within a closed group of subscribers to their security alert service. In the standard model, only good guys are allowed to join the club*

## **-[8]Cyber Insurance**

*Cyber-insurance is among the oldest proposals for market mechanisms to overcome the security market failure.*

*The logic that cures the market failure goes as follows: end users demand insurance against financial losses from*

*information security breaches and insurance companies sell this kind of coverage after a security audit. The premium is assumed to be adjusted by the individual risk, which depends on the IT systems in use and the security mechanisms in place.*

Let's try define the market's participants, their expectations and value added through their actions, if any, of

course.

## **Buyers**

-[9]malicious (E-criminals, malware authors, competitors, political organization/fraction etc.)

-third party, end users, private detectives, military, intelligence personnel

-vendors (either through intermediary, or directly themselves, which hasn't actually happened so far)

## **Sellers**



- reputable
- newly born
- questionable
- does it matter at the bottom line?

## **Intermediaries**

- [10]iDefense
- [11]ZeroDayInitiative-[12]Digital Armaments

## **Society**

- Internet
- CERT model - totally out of the game these days?

215

As iDefense simply had to restore their position in this emerging market developed mainly by them, an offer for [13] \$10,000 was made for a critical vulnerability as defined by Microsoft. I mean, I'm sort of missing the point in here. Obviously, they are aware of the level of quality research that could be sold to them.

Still I wonder what exactly are they competing with :

- trying to attract the most talented researchers, instead of having them turn to the dark side? I doubt they are that much socially oriented, but still it's an option?
- ensuring the proactive security of its customers through first notifying them, and then the general

public? That doesn't necessarily secure the Internet, and sort of provides the clientele with a false feeling of

security, "what if" a (malicious) vulnerability researcher doesn't cooperate with iDefense, and instead sells an 0day to a competitor? Would the vendor's IPS protect against a threat like that too?

- fighting against the permanent opportunity of another 0day, gaining only a temporary momentum advantage?

- improving the company's clients list through constant collaboration with leading vendors while communicating a vulnerability in their software products?

A lot of [14]research [15]publications reasonably argue that the credit for the highest social-welfare return

goes to a CERT type of a model. And while this is truly, accountability and providing a researcher with the highest,

both tangible, and intangible reward for them is what also can make an impact. As a matter of fact, is blackmailing a

nasty option that could easily become reality in here, or I'm just being paranoid?

To conclude, this very same shop is definitely among the many other active out there for sure, so, sooner or

later we would either witness the introduction of a reputable Auction based vulnerabilities market model, or

continue living with windows of opportunities, clumsy vendors, and 0day mom-and-dad shops :) But mind you,

turning vuln research into IP and paying for it would provide enough motivation for an underground 0day as well,

wouldn't it?

### **14.03.2006**

OSVDB's Blog - [16]Where's my 0day, please?

OSVDB's Blog - [17]Vulnerability Markets

216

### **11.03.2006**

LinuxSecurity.com - [18]Where's my 0day, please?

FIRST - [19]Where's my 0day, please?

### **10.03.2006** - Sites that picked up the story :

Net-Security.org - [20]Where's my 0day, please?

MalwareHelp.org- [21]The International Exploits Shop:  
Where's my 0day, please?

Security.nl - [22]Internationale Exploit Shop levert 0days op bestelling

WhiteDust.net - [23]Where's my 0day, please?

Reseaux-Telecoms.net - [24]Danchev sur l'Achat de failles

Informit Network - [25]0-Days for Sale

**09.03.2006** - Two nice articles related to the issue appeared yesterday as well, "[26]Black market thrives on vulnerability trading", from the article :

*"Security giant Symantec claims that anonymous collusion between hackers and criminals is creating a thriving*

*black market for vulnerability trading. As criminals have woken up to the massive reach afforded to their activities thanks to the Internet, hackers too are now able to avoid risking prison sentences by simply selling on their findings.*

*Graeme Pinkney, a manager at Symantec for trend analysis, told us: 'People have suddenly realised that there's now*

*a profit margin and a revenue stream in vulnerabilities... There's an element of anonymous co-operation between the hacker and criminal.'*"

and "[27]The value of vulnerabilities", a quote :

*" There are no guarantees, and therefore I think it would be pretty naive to believe that the person reporting*

*the issue is the only one aware of its existence. That in itself is pretty frightening if you think about it. "*

Technorati tags:

[28]Security, [29]0day, [30]0bay, [31]Vulnerabilities, [32]Exploits, [33]iDefense, [34]ZeroDayInitiative, [35]Digital

Armaments

1. <http://www.xshop.in/>

2. <http://ddanchev.blogspot.com/2005/12/0bay-how-realistic-is-market-for.html>

3. [http://photos1.blogger.com/blogger/1933/1779/1600/International\\_Exploits\\_Shop.1.jpg](http://photos1.blogger.com/blogger/1933/1779/1600/International_Exploits_Shop.1.jpg)
4. <http://koffix.com/research/sites/xshop.in.html>
5. [http://photos1.blogger.com/blogger/1933/1779/1600/International\\_Exploits\\_Shop%20-%20Products2.jpg](http://photos1.blogger.com/blogger/1933/1779/1600/International_Exploits_Shop%20-%20Products2.jpg)
6. [http://photos1.blogger.com/blogger/1933/1779/1600/International\\_Exploits\\_Shop%20-%20Products1.jpg](http://photos1.blogger.com/blogger/1933/1779/1600/International_Exploits_Shop%20-%20Products1.jpg)
7. [http://events.ccc.de/congress/2005/fahrplan/attachments/542-Boehme2005\\_22C3\\_VulnerabilityMarkets.pdf](http://events.ccc.de/congress/2005/fahrplan/attachments/542-Boehme2005_22C3_VulnerabilityMarkets.pdf)
8. <http://infosecon.net/workshop/pdf/15.pdf>
9. <http://ddanchev.blogspot.com/2006/01/was-wmf-vulnerability-purchased-for.html>
10. <http://www.idefense.com/>
11. <http://www.zerodayinitiative.com/>
12. <http://www.digitalarmaments.com/>
13. <http://ddanchev.blogspot.com/2006/02/how-to-win-10000-bucks-until-end-of.html>
14. <http://www.dtc.umn.edu/weis2004/kannan-telang.pdf>
15. [http://mansci.pubs.informs.org/e\\_companion\\_pages/May\\_05\\_EC/Kanan\\_Telang\\_EC.pdf](http://mansci.pubs.informs.org/e_companion_pages/May_05_EC/Kanan_Telang_EC.pdf)

16. <http://www.osvdb.org/blog/?p=101>
17. <http://www.osvdb.org/blog/?p=102>
18. <http://www.linuxsecurity.com/content/view/121889/65/>
19. <http://www.first.org/newsroom/globalsecurity/9825.html>
20. <http://net-security.org/news.php?id=10467>
21. <http://www.malwarehelp.org/news/article-2886.html>
22. [http://www.security.nl/article/13099/1/Internationale\\_Exploit\\_Shop\\_levert\\_0days\\_op\\_bestelling.html](http://www.security.nl/article/13099/1/Internationale_Exploit_Shop_levert_0days_op_bestelling.html)
23. <http://www.whitedust.net/speaks/2263/>
24. <http://www.reseaux-telecoms.net/actualites/lire-danchev-sur-l-achat-de-failles-12703.html?pid=6>
25. <http://www.informit.com/discussion/index.asp?postid=f8857a10-149e-4c50-b7c0-243a82a8bd47&rl=1>
26. <http://www.pcpro.co.uk/news/84523/black-market-thrives-on-vulnerability-trading.html>
27. <http://www.securityfocus.com/columnists/391>
28. <http://technorati.com/tag/Security>
29. <http://technorati.com/tag/0day>
30. <http://technorati.com/tag/0bay>
31. <http://technorati.com/tag/Vulnerabilities>
32. <http://technorati.com/tag/Exploits>

- 33. <http://technorati.com/tag/iDefense>
- 34. <http://technorati.com/tag/ZeroDayInitiative>
- 35. <http://technorati.com/tag/Digital+Armaments>

218

### **DVD of the Weekend - The Immortals (2006-03-10 14:23)**

[1]The Lawnmower Man : Beyond Cyberspace was among the [2]several [3]other classic [4]techno thrillers I was

watching and mostly remembering pleasant times from the past. I actually got in touch with [5]SFAM from the

[6]CyberpunkReview.com, and intend to contribute with another point of view to his initiative I highly recommend

you to keep an eye on.

This weekend, I want to recommend you one of the best European film productions ever, namely [7]Enki Bi-

lal's [8]adaptation of his [9]Nikopol Trilogy - [10]The Immortals.

Here's an excerpt from a review, and another [11]one :

*"New York City, year 2095. A floating pyramid has emerged in the skies above, inhabited by ancient Egyptian Gods.*

*They have cast judgment down upon Horus, one of their own. Now he must find a human host body to inhabit, and*

*search for a mate to continue his own life. Below, a beautiful young woman with blue hair, blue tears and a power*

*even unknown to her, wanders the city in search of her identity. Reality in this world has a whole new meaning as bodies, voices and memories converge with Gods, mutants, extra-terrestrials and mortals."*

[12]

[13]The Matrix did shock, and set a new benchmark by combining Hollywood's passion for entertainment,

and [14]Japan's [15]culture, still, European productions such as the [16]5th Element, and [17]The Immortals, are on

my hall of fame for effects and the stories themselves. Enjoy it!

Technorati tags :

[18]Lone Gunmen, [19]The Outer Limits, [20]Lawnmower Man, [21]Immortals, [22]Enki Bilal, [23]Nikopol Trilogy,

[24]Techno Thriller, [25]Cyberpunk

1. <http://ddanchev.blogspot.com/2006/03/dvd-of-past-weekend.html>

2. <http://ddanchev.blogspot.com/2006/02/dvd-of-weekend-lone-gunmen.html>

3. <http://ddanchev.blogspot.com/2006/02/dvd-of-weekend-outer-limits-sex-and.html>

4. <http://en.wikipedia.org/wiki/Techno-thriller>

5. <http://www.blogger.com/comment.g?blogID=18493443&postID=114164907056399632>



6. <http://www.cyberpunkreview.com/>
  7. <http://bilal.enki.free.fr/>
  8. <http://www.mediadis.com/video/detail.asp?id=138924>
  9. [http://en.wikipedia.org/wiki/La\\_Foire\\_aux\\_immortels](http://en.wikipedia.org/wiki/La_Foire_aux_immortels)
  10. [http://en.wikipedia.org/wiki/Immortel\\_\(Ad\\_Vitam\)](http://en.wikipedia.org/wiki/Immortel_(Ad_Vitam))
  11. [http://www.fi-sci.net/index.php?option=com\\_content&task=view&id=589&Itemid=71](http://www.fi-sci.net/index.php?option=com_content&task=view&id=589&Itemid=71)
  12. [http://photos1.blogger.com/blogger/1933/1779/1600/immortals\\_the\\_movie\\_2.0.jpg](http://photos1.blogger.com/blogger/1933/1779/1600/immortals_the_movie_2.0.jpg)
  13. <http://whatisthematrix.warnerbros.com/>
  14. <http://en.wikipedia.org/wiki/Anime>
  15. <http://en.wikipedia.org/wiki/Cyberpunk>
  16. <http://www.geocities.com/Hollywood/Set/8452/5thelement.html>
  17. [http://en.wikipedia.org/wiki/Immortel\\_\(Ad\\_Vitam\)](http://en.wikipedia.org/wiki/Immortel_(Ad_Vitam))
- 219
18. <http://technorati.com/tag/Lone+Gunmen>
  19. <http://technorati.com/tag/The+Outher+Limits>
  20. <http://technorati.com/tag/Lawnmower+Man>
  21. <http://technorati.com/tag/Immortals>

- 22. <http://technorati.com/tag/Enki+Bilal>
- 23. <http://technorati.com/tag/Nikopol+Trilogy>
- 24. <http://technorati.com/tag/Techno+Thriller>
- 25. <http://technorati.com/tag/Cyberpunk>

220

### **Security vs Privacy or what's left from it (2006-03-15 12:41)**

My latest privacy related posts had to do with "[1]The Future of Privacy = don't over-empower the watchers!" and

"[2]Data mining, terrorism and security" in respect to the the still active TIA and the hopes for the effectiveness out of data mining. While these are important topics I feel every decent citizen living in the 21st century should be aware

of - many still "think conspiracies" than real-life scenarios. At the bottom line, privacy violations for the sake of your security and civil liberties are a common event these days!

Today, I came across an article "[3]Google must capitulate to DoJ, says judge" in [4]relation [5]to the DoJ's subpoena trying to get access to random sites and searches in order to justify its statement that anti-porn filters do not

protect young children online.

The NYtimes is also a running a story on [6]this. What I truly liked is US District Judge James Ware's comment

that he was reluctant to give the Justice Department everything it wanted because of the "perception by the public

that this is subject to government scrutiny" when they type search terms into Google.com, that's right, but you would be also right to conclude that such requests would turn into a habit given Google's data aggregation power. It's s a

complex process to run the world's most popular search engine when everyone wants to take a bite from you, at

least they have hell of motto to sort of guide them in future situations like this, but is it?

This time it's a misjudged online porn request that gets approved, next time, it would be Google against [7]the

[8]terrorists, again, for the sake of your Security, one backed up by a little bit of glue as on the majority of occasions!

Technorati tags :

[9]Privacy, [10]Google, [11]Search Engine

1. <http://ddanchev.blogspot.com/2006/03/future-of-privacy-dont-over-empower.html>
2. <http://ddanchev.blogspot.com/2006/03/data-mining-terrorism-and-security.html>
3. <http://networks.silicon.com/webwatch/0,39024667,39157220,00.htm>
4. <http://ddanchev.blogspot.com/2006/01/still-worry-about-your-search-history.html>
5. <http://ddanchev.blogspot.com/2006/01/feds-google-msns-reaction-and-how-you.html>

6.

<http://www.nytimes.com/2006/03/15/technology/15google.html?ex=1300078800&en=c701e37ac929f3dc&ei=5090&partner=rssuserland&emc=rss>

7. <http://ddanchev.blogspot.com/2006/01/cyberterrorism-recent-developments.html>

8. <http://ddanchev.blogspot.com/2005/12/cyberterrorism-dont-stereotype-and-its.html>

9. <http://technorati.com/tag/Privacy>

10. <http://technorati.com/tag/Google>

11. <http://technorati.com/tag/Search+Engine>

221

## **Old physical security threats still working (2006-03-16 17:50)**

In "[1]The Complete Windows Trojans Paper" that I released back in 2003 (you can also update yourself with some

[2]recent [3]malware trends!) I briefly mentioned on the following possibility as far as physical security and malware

was concerned :

*"Another way of infecting while having physical access is the Auto-Starting CD function. You've probably no-*

*ticed that when you place a CD in your CDRom, it automatically starts with some setup interface; here's an example*

*of the Autorun.inf file that is placed on such CD's:*

*[autorun]open=setup.exeicon=setup.exe So you can imagine that while running the real setup program a trojan could*

*be run VERY easily, and as most of you probably don't know about this CD function they will get infected and won't*

*understand what happened and how it's been done. Yeah, I know it's convenient to have the setup.exe autostart but*

*security is what really matters here, that's why you should turn off the Auto-Start functionality by doing the following: Start Button -> Settings -> Control Panel -> System -> Device Manager -> CDROM -> Properties -> Settings"*

*and another interesting point :*

*"I know of another story regarding this problem. It's about a Gaming Magazine that used to include a CD*

*with free demo versions of the latest games in each new edition. The editors made a contest to find new talents and*

*give the people programming games the chance to popularise their productions by sending them to the Editors. An*

*attacker infected his game with a new and private trojan and sent it to the Magazine. In the next edition the "game"*

*appeared on the CD and you can imagine the chaos that set in."*

Things have greatly changed for the last three years, while it may seem that global malware outbreaks are the

dominant trend, slow worms, 0day malware and any other "beneath the AVs radar" concepts seem to be the next pattern.

It's "great" to find out that age-old CD trick seems to be fully working, whereas I can't reckon someone was

saying "Hello World" to [4]WMF's back then! TechWorld wrote a great article two days ago titled "[5]Workers duped by simple CD ruse", an excerpt :

*" To office workers trudging to their cubicles, the promotion looked like a chance at sweet relief from the five-day-a-week grind. By simply running a free CD on their computers, they would have a chance to win a vacation. But*

*the beguiling morning giveaway in London's financial district last month was more nefarious than it appeared. When*

*a user ran the disc, the code on it prompted a browser window that opened a Web site, Chapman said. The site then*

*tried to load an image from another Web site, Chapman said. "*

While we can argue how vulnerable to security threats and end user is these days, compared to physical secu-

222

rity ones, there are lots of [6]cases [7]pointing out the targeted nature of attacks, and the simple diversification of attack methods from what is commonly accepted as current trend. My point is that if you believe the majority of

threats are online based ones, someone will exploit this attitude of yours and target you physically.

And while I feel the overall state of physical security in respect to end users and their workstations has greatly

improved with initiatives such as ensuring the host's integrity and IPSs, what you should consider taking care of is

-

who is capable of peeping behind your back and what effect may it have on any of your projects? [8]3M's Privacy

Filters are a necessity these days, and an alternative to the obvious [9]C.H.I.M.P. (monitor mirror). Be aware!

**UPDATE** - this post recently appeared at LinuxSecurity.com - [10]Old physical security threats still working

More resources on physical security can also be found at :

[11]19 Ways to Build Physical Security into a Data Center

[12]Securing Physical Access and Environmental Services for Datacenters

[13]CISSP Physical Security Exam Notes

[14]Physical Security 101

[15]SANS Reading Room's Physical Security section

Technorati tags :

[16]Security, [17]Physical Security, [18]Workplace

1.

[http://www.windowsecurity.com/whitepapers/The\\_Complete\\_](http://www.windowsecurity.com/whitepapers/The_Complete_)

[Windows\\_Trojans\\_Paper.html](#)

2. <http://ddanchev.blogspot.com/2006/02/recent-malware-developments.html>

3. <http://ddanchev.blogspot.com/2006/01/malware-future-trends.html>

4. <http://ddanchev.blogspot.com/2006/01/was-wmf-vulnerability-purchased-for.html>

5. <http://www.techworld.com/security/news/index.cfm?NewsID=5563>

6. <http://arik.baratz.org/wordpress/2005-05-29/trojan-horses-abound>

7. [http://www.newsfactor.com/story.xhtml?story\\_id=41980](http://www.newsfactor.com/story.xhtml?story_id=41980)

8. [http://www.3m.com/us/office/myworkspace/mon\\_filters\\_privacy.jhtml](http://www.3m.com/us/office/myworkspace/mon_filters_privacy.jhtml)

9. <http://www.thinkgeek.com/computing/accessories/2940/>

10. <http://www.linuxsecurity.com/content/view/122000/65/>

11. <http://www.csoonline.com/read/110105/datacenter.html>

12. [http://www.infosecwriters.com/text\\_resources/pdf/datacenter\\_security.pdf](http://www.infosecwriters.com/text_resources/pdf/datacenter_security.pdf)

13. [http://home.pacific.net.hk/~kplab/CISSP\\_Exam\\_Notes\\_Physical\\_Security\\_v1.1.pdf](http://home.pacific.net.hk/~kplab/CISSP_Exam_Notes_Physical_Security_v1.1.pdf)



14. <http://csrc.nist.gov/cryptval/physec/papers/physecpaper05.pdf>
15. <http://www.sans.org/rr/whitepapers/physcial/>
16. <http://technorati.com/tag/Security>
17. <http://technorati.com/tag/Physical+Security>
18. <http://technorati.com/tag/Workplace>

223

### **Getting paid for getting hacked (2006-03-17 13:19)**

In the middle of February, Time Magazine ran a great article on Cyberinsurance or "[1]Shock Absorbers", and I feel this future trend deserves a couple of comments, from the article :

*"As companies grow more dependent on the Internet to conduct business, they have been driving the growing*

*demand for cyber insurance. Written premiums have climbed from \$100 million in 2003 to \$200 million in 2005,*

*according to Aon Financial Services Group. The need for cyberinsurance has only increased as hacker move away*

*from general mischief to targeted crimes for profit. Insurers offer two basic types of cyber insurance: first-party*

*coverage will help companies pay for recovery after an attack or even to pay the extortion for threatened attacks,*

*while third-party coverage helps pay legal expenses if someone sues after a security breach. Demand for*

*insurance*

*is also driven by laws in over twenty states that require companies to notify consumers if a breach compromises their personal data. However, prevention is still the top priority for most companies, since loss of critical data to competitors would do damage beyond the payout of any policy."*

[2]Cyber insurance seems to be an exciting business with a lot of uncertainty compared to other industries

with more detailed ROIs, as I feel the information security one is missing a reliable [3]ROSI model. I once blogged

about [4]why we cannot measure the real cost of cybercrime, and commented the same issue with the "[5]FBI's 2005

Computer Crime Survey - what's to consider?". Don't get me wrong, these are reliable sources for various market

indicators, still the situation is, of course, even worse.

But how do you try to value security at the bottom line?

Bargaining with security, and negotiating its cost is projectable and easy to calculate, but whether security is

actually in place or somehow improved, seems to be a second priority - bad bargaining in the long-term, but

marketable one in the short one.

Going back to the article, I hope there aren't any [6]botnet herders reading this, especially the first-party cov-

erage point. To a certain extend, that's a very pointless service, as it fuels the growth of [7]DDoS extortion, as now

it's the insurer having to pay for it, meaning there're a lot of revenue streams to be taken by the cybergang. While

covering the expenses of extortion attempts is very marketable, it clearly highlights how immature the current state

of the concept really is. Something else to consider, is that a lot of companies reasonably take advantage of MSSPs

with the idea to forward risk/outsource their security to an experienced provider, and most importantly, budget with

their security spending. And while the [8]California's SB 1386 is important factor for growth of the service given the

20 states participating, with the number of [9]stolen databases from both, commercial, educational and [10]military

organizations, insurers will start earning a lot of revenues that could have been perhaps spent in security R &D -

which I doubt they would spend them on, would they?

## **UPDATE:**

224

The post has just appeared at Net-Security.org - "[11]Getting paid for getting hacked", as well as LinuxSecurity.com -

"[12]Getting paid for getting hacked"

Related resources :

[13]Cyber-Insurance Revisited

[14]Economics and Security Resource Page

[15]WEIS05 WorkShop on Economics and Information Security - papers and presentations

[16]Valuing Security Products and Patches

[17]The New Economics of Information Security

[18]Safety at a Premium

[19]Cyber Insurance and IT Security Investment Impact on Interdependent Risk

[20]Valuing Security Products and Patches

[21]Network Risks, Exposures and Solutions

Technorati tags :

[22]Security, [23]ROSI, [24]Cyber Insurance, [25]Economics

1. <http://www.time.com/time/insidebiz/article/0,9171,1156596,00.html>

2. <http://www.ecommercetimes.com/story/35045.html>

3. <http://www.cio.com/archive/021502/security.html>

4. <http://ddanchev.blogspot.com/2006/01/why-we-cannot-measure-real-cost-of.html>

5. <http://ddanchev.blogspot.com/2006/01/fbis-2005-computer-crime-survey-whats.html>

6. <http://ddanchev.blogspot.com/2006/01/what-are-botnet-herds-up-to.html>
7. <http://ddanchev.blogspot.com/2006/02/war-against-botnets-and-ddos-attacks.html>
8. [http://info.sen.ca.gov/pub/01-02/bill/sen/sb\\_1351-1400/sb\\_1386\\_bill\\_20020926\\_chaptered.html](http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html)
9. <http://ddanchev.blogspot.com/2006/01/personal-data-security-breaches.html>
10. <http://ddanchev.blogspot.com/2006/01/insecure-irony.html>
11. <http://net-security.org/news.php?id=10604>
12. <http://www.linuxsecurity.com/content/view/122019/65/>
13. <http://infosecon.net/workshop/pdf/15.pdf>
14. <http://www.cl.cam.ac.uk/~rja14/econsec.html>
15. <http://infosecon.net/workshop/schedule.php>
16. <http://www.citi.umich.edu/u/rwash/projects/econsec/valuesec-rwash-stiet.pdf>
17. <http://www.financetech.com/printableArticle.jhtml;jsessionid=T4JKDVMMLWIPYQSNDBCSKHSCJUMKJVN?articleID=18901266>
18. <http://www.csoonline.com/read/120902/safety.html>
19. <http://infosecon.net/workshop/pdf/56.pdf>

20.

<http://www.citi.umich.edu/u/rwash/projects/econsec/valuesec-rwash-stiet.pdf>

21.

[http://www.aon.com/us/about/events/pdf/tech\\_week\\_network\\_risk\\_presentation.pdf](http://www.aon.com/us/about/events/pdf/tech_week_network_risk_presentation.pdf)

22. <http://technorati.com/tag/Security>

23. <http://technorati.com/tag/ROSI>

24. <http://technorati.com/tag/Cyber+Insurance>

25. <http://technorati.com/tag/Economics>

225

### **"Successful" communication (2006-03-17 14:39)**

[1]You know [2]Dilbert, don't you? I find this cartoon a very good representation of what is going on in the

[3]emerging [4]market [5]for [6]software [7]vulnerabilities, and of course, its [8]OTC [9]trade [10]practices - total

miscommunication and different needs and opinions. While different opinions and needs provoke quality discussion

and I understand the point that everyone is witnessing that something huge is happening, "so why shouldn't I?", but at the bottom line, it's so obvious that there isn't any sort of mission or social welfare goal to be achieved, that everyone is commercializing what used to be the "information wants to be free" attitude.

Weren't software vulnerabilities supposed to turn into a commodity given the number of people capable and

actually discovering them, where "windows of opportunities" get the highest priority as a con? That is, compared to

[11]commercializing vulnerability research, empowering researchers to the skies, and turning vulnerabilities into an

IP, totally decentralizing the current sources of information, and fueling the growth of underground models, as it's

obvious that for the time being vulnerabilities and their early acquirement seems to be where the \$ is. What do you

think?

Technorati tags :

[12]Security, [13]Vulnerabilities, [14]0day, [15]0bay, [16]Dilbert

1. <http://photos1.blogger.com/blogger/1933/1779/1600/dilbert20060121046729.1.jpg>
2. <http://www.unitedmedia.com/comics/dilbert/>
3. <http://osvdb.org/blog/?p=102>
4. [http://blogs.technet.com/ms\\_schweiz\\_security\\_blog/archive/2006/03/17/422292.aspx](http://blogs.technet.com/ms_schweiz_security_blog/archive/2006/03/17/422292.aspx)
5. <http://osvdb.org/blog/?p=105>
6. <http://osvdb.org/blog/?p=106>
7. <http://ddanchev.blogspot.com/2005/12/0bay-how-realistic-is-market-for.html>

8. [http://en.wikipedia.org/wiki/Over-the-counter\\_\(finance\)](http://en.wikipedia.org/wiki/Over-the-counter_(finance))
9. <http://ddanchev.blogspot.com/2006/01/was-wmf-vulnerability-purchased-for.html>
10. <http://ddanchev.blogspot.com/2006/03/wheres-my-0day-please.html>
11. <http://ddanchev.blogspot.com/2006/02/how-to-win-10000-bucks-until-end-of.html>
12. <http://technorati.com/tag/Security>
13. <http://technorati.com/tag/Vulnerabilities>
14. <http://technorati.com/tag/0day>
15. <http://technorati.com/tag/0bay>
16. <http://technorati.com/tag/Dilbert>

226

### **Is a Space Warfare arms race really coming? (2006-03-20 21:47)**

In one of my previous posts "[1]Who needs nuclear weapons anymore?" I was emphasizing on another, much

more assymetric, still dangerous alternative, [2]EMP weapons. I came across to a recent Boston.com article titled

"[3]Pentagon eyeing weapons in space" that's gives a relevant overview of the current state of the U.S's ambitions, an excerpt :

*" The Pentagon is asking Congress for hundreds of millions of dollars to test weapons in space, marking the*



*biggest step toward creating a space battlefield since President Reagan's long-defunct [4]"star wars" project during the Cold War, according to federal budget documents. "*

as well as some of the projects the request is going to be spent on :

*-" One \$207 million project by the Missile Defense Agency features experiments on micro-satellites, including*

*using one as a target for missiles. This experiment "is particularly troublesome," according to the joint report, "as it would be a de-facto antisatellite test." "*

*-"A project description says the Air Force would test a variety of powerful laser beams "for applications including antisatellite weapons. "*

*-" The agency also has asked Congress for \$220 million for "Multiple Kill Vehicles," a program that experts say could be proposed as a space-based missile interceptor. "*

*-" Meanwhile, the Air Force wants \$33 million for the Hypersonic Technology Vehicle, envisioned as space vehicle capable of delivering a military payload anywhere on earth within an hour, according to an official project description. "*

Big government contractors(the majority of and past revenues secured by government contracts) such as [5]Northrop

Grumman and [6]Lockhead Martin are more than eager to get hold of implementing these projects and launching

them into space.

I highly recommend you to read [7]Space Warfare  
Foolosophy: Should the United States be the First Country  
to Weaponize Space? if you want to go through a very good  
point of view – it's all about politics and who feels like  
getting superior. An [8]arms race is slowly emerging, and  
that's the distrurbing part!

As a matter of fact, SFAM from the [9]CyberpunkReview.com  
has recently featured a review of one of the

best X-files episodes "[10]Kill Switch" where the main  
characters try to escape an AI playing with leftover Star  
Wars military orbital lasers .

227

More resources can also be found at :

[11]Orbital Weaponry

[12]Space Based Weapons

[13]Space Warfare Weapons

[14]SpaceWar.com

[15]Militarization and Weaponization of Space

[16]Space and Electronifc Warfare (ELINT) Lexicon

[17]Gyre's Space Warfare section

[18]Directed Energy Warfare – Space Age Weapons

- [19]Secret Orbiter System Revealed
- [20]Military Transformation Uplink: March 2006
- [21]Anti-Satellite Weapons
- [22]Military Space Programs
- [23]Space Weapons For Earth Wars
- [24]The Revolution in War (227 pages)
- [25]A Political Strategy for Antisatellite Weaponry
- [26]Space Weapons - Crossing the U.S Rubicon
- [27]Preventing the Weaponization of Space
- [28]Space Weapons: The Urgent Debate
- [29]Satellite Killers and Space Dominance
- [30]The Advent of Space Weapons
- [31]US Space Command Vision for 2020
- [32]China's Space Capabilities and the Strategic Logic of Anti-Satellite Weapons
- [33]U.S. Air Force Plans for Future War in Space - 2004
- [34]Space Warfare in Perspective - 1982

Technorati tags :

[35]EMP, [36]Nuclear, [37]War, [38]Space, [39]Space Warfare, [40]Space Weapons, [41]Security

1. <http://ddanchev.blogspot.com/2006/02/who-needs-nuclear-weapons-anymore.html>
2. [http://en.wikipedia.org/wiki/Electromagnetic\\_pulse](http://en.wikipedia.org/wiki/Electromagnetic_pulse)
3. [http://www.boston.com/news/nation/articles/2006/03/14/pentagon\\_eyeing\\_weapons\\_in\\_space/](http://www.boston.com/news/nation/articles/2006/03/14/pentagon_eyeing_weapons_in_space/)
4. [http://en.wikipedia.org/wiki/Strategic\\_Defense\\_Initiative](http://en.wikipedia.org/wiki/Strategic_Defense_Initiative)
5. [http://www.is.northropgrumman.com/products/dod\\_products/cwin.html](http://www.is.northropgrumman.com/products/dod_products/cwin.html)
6. <http://www.lockheedmartin.com/>
7. <http://www.airpower.maxwell.af.mil/airchronicles/cc/koskinas.html>
8. [http://en.wikipedia.org/wiki/Arms\\_race](http://en.wikipedia.org/wiki/Arms_race)
9. <http://www.cyberpunkreview.com/>
10. <http://www.cyberpunkreview.com/movie/decade/1990-1999/x-files-kill-switch-episode-11-season-5/>
11. [http://en.wikipedia.org/wiki/Orbital\\_weaponry](http://en.wikipedia.org/wiki/Orbital_weaponry)
12. <http://www.au.af.mil/au/aul/school/sncoa/spacebw.htm>
13. [http://www.historyofwar.org/articles/concepts\\_spacewar.html](http://www.historyofwar.org/articles/concepts_spacewar.html)
14. <http://www.spacewar.com/>
15. <http://grant.henninger.name/space/>

16. <http://www.sew-lexicon.com/>
17. <http://www.gyre.org/news/Space%20Warfare>
18. <http://aussiethule.blogspot.com/2006/03/directed-energy-warfare-space-age.html>
19. [http://americanthinker.com/articles.php?article\\_id=5306](http://americanthinker.com/articles.php?article_id=5306)
20. <http://www.windsofchange.net/archives/008175.php#008175>
21. <http://www.fas.org/spp/military/program/asat/index.html>
22. <http://www.fas.org/spp/military/program/index.html>
23. [http://www.space.com/business/technology/technology/space\\_war\\_020515-1.html](http://www.space.com/business/technology/technology/space_war_020515-1.html)
24. <http://www.csbaonline.org/4Publications/Archive/R.20041201.RevInWar/R.20041201.RevInWar.pdf>
25. <http://www.ndu.edu/library/ic6/93A106.pdf>
26. <http://www.fas.org/RLG/041100-rubicon.pdf>
27. <http://www.pugwashgroup.ca/events/documents/2003/report-05-27-03.pdf>
28. <http://www.student-pugwash.org/halifax2003/papers/Marshall.pdf>

29. <http://www.spokesmanbooks.com/Spokesman/PDF/Aldridge.pdf>
30. [http://www.cfr.org/content/publications/attachments/Bergman\\_11ast03.pdf](http://www.cfr.org/content/publications/attachments/Bergman_11ast03.pdf)
31. <http://www.fas.org/spp/military/docops/usspac/visbook.pdf>
32. <http://cns.miis.edu/pubs/week/020722.htm>
33. [http://www.space.com/business/technology/technology/higher\\_ground\\_040222.html](http://www.space.com/business/technology/technology/higher_ground_040222.html)
34. <http://www.airpower.maxwell.af.mil/airchronicles/aureview/1982/jul-aug/humble.html>
35. <http://technorati.com/tag/EMP>
36. <http://technorati.com/tag/Nuclear>
37. <http://technorati.com/tag/War>
38. <http://technorati.com/tag/Space>
39. <http://technorati.com/tag/Space+Warfare>
40. <http://technorati.com/tag/Space+Weapons>
41. <http://technorati.com/tag/Security>

## **The Practical Complexities of Adware Advertising (2006-03-21 13:10)**

A report [1]released by the The Center for Democracy and Technology yesterday, "[2]How Advertising Dollars

Encourage Nuisance and Harmful Adware and What Can be Done to Reverse the Trend", outlines the practical

complexities of Adware Advertising. It gives a great overview of the parties involved, discusses a case study "CDT

engages the advertisers", as well as outlines a possible solution, namely Adoption and Enforcement of Advertising

Placement Policies. Here's a excerpt from the research findings :

*" At this point, CDT has set a low bar by merely asking a small group of companies to contact us to discuss*

*their advertising policies in the context of nuisance and harmful adware. We are working to increase awareness*

*of the complex business models associated with nuisance and harmful adware, and we are pointing advertisers to*

*policies and criteria that already exist as a step towards creating and enforcing their own policies. It is also imperative that advertising networks engage in self-regulation in order to aid in this endeavor. Initiatives such as the TRUSTe Trusted Download Program can help to set certification standards and provide public criteria for evaluating adware*

*makers. Advertisers must demand strict compliance from their affiliates and refuse to work with blind networks and*

*other networks that cannot commit to following stringent advertising policies. Without advertising dollars, there*

*would be no nuisance or harmful adware. CDT is committed to working with advertisers to stem the tide of this*

*nefarious form of software. "*

Now, if major advertising platforms start measuring the [3]maliciousness of the Web, namely evaluate the par-

ticipants' condition on a regular basis, they will lose the scale necessary for generating the billions of dollars

necessary to, sort of, live with [4]click-fraud. In respect to future [5]online advertising trends, I feel that cost per performance/action model, would sooner or later emerge, given the successful collective bargaining of all the sites

participating – I really hope so!

How it would influence Google's ability to perform financially, contribute to the growth of Web 2.0, being

among the few companies born in, is yet another topic to speculate on. As a matter of fact, Google recently launched

[6]Google Finance, still I miss what's all the buzz all about as compared to [7]Yahoo's Finance Google still has a lot of job to do, given they actually want to turn and position themselves as Yahoo! 2.0 in respect to turning into a Internet

Portal – which I doubt as they tend to be rather productive while disrupting.



Great [8]report, so consider going through it. And, in case you're interested in learning more about the different spyware/adware legislations, current and future trends, you can also check [9]Ben Edelman's and [10]Eric Goldman's outstanding research on the topic.

The post recently appeared at Net-Security.org - "[11]The practical complexities of adware advertising"

More resources can also be found at :

230

[12]Spyware/Adware Podcasts

[13]Top 10 Anti Spyware Apps reviewed

[14]Clean and Infected File Sharing Programs

Technorati tags :

[15]Security, [16]Spyware, [17]Adware, [18]Advertising, [19]Center for Democracy and Technology

1. <http://www.cdt.org/press/20060320adwarerelease.pdf>

2. <http://www.cdt.org/privacy/20060320adware.pdf>

3. <http://ddanchev.blogspot.com/2006/02/look-whos-gonna-cash-for-evaluating.html>

4. <http://www.wired.com/wired/archive/14.01/fraud.html>

5. [http://www.businessweek.com/magazine/content/06\\_13/b3977401.htm](http://www.businessweek.com/magazine/content/06_13/b3977401.htm)

6. <http://finance.google.com/finance>
7. <http://finance.yahoo.com/>
8. <http://www.cdt.org/privacy/20060320adware.pdf>
9. <http://www.benedelman.org/>
10. <http://blog.ericgoldman.org/>
11. <http://net-security.org/news.php?id=10640>
12. <http://thoughtshapers.com/index.php/weblog/benedelmanpodcasts>
13. [http://reviews.cnet.com/4520-3688\\_7-6456087-1.html](http://reviews.cnet.com/4520-3688_7-6456087-1.html)
14. <http://www.spywareinfo.com/articles/p2p/>
15. <http://technorati.com/tag/Security>
16. <http://technorati.com/tag/Spyware>
17. <http://technorati.com/tag/Adware>
18. <http://technorati.com/tag/Advertising>
19. <http://technorati.com/tag/Center+for+Democracy+and+Technology>

231

**Privacy issues related to mobile and wireless Internet access (2006-03-21 17:24)**

[1]I just came across a research worth checking out by all the [2]wardrivers and mobile/wireless Internet users out

there. While it's written in 2004, "[3]Privacy, Control and Internet Mobility", provides relevant info on an important topic - what kind of information is leaking and how can this be reduced. The abstract describes it as :

*" This position paper explores privacy issues created by mobile and wireless Internet access. We consider the*

*information about the users identity, location, and the serviced accessed that is necessarily or unnecessarily revealed observers, including the access network, intermediaries within the Internet, and the peer endpoints. In particular, we are interested in data that can be collected from packet headers and signaling messages and exploited to control*

*the users access to communications resources and online services. We also suggest some solutions to reduce the*

*amount of information that is leaked. "*

A more in-depth overview on the topic can also be found in "[4]A Framework for Location Privacy in Wireless

Networks", an excerpt :

*" For example, even if an anonymous routing protocol such as [5] ANODR is used, an attacker can track a user's location through each connection, and associate multiple connections with the same user. When the user arrives*

*at home, she will have left a trail of packet crumbs which can be used to determine her identity. In this paper, we*

*explore some of the possible requirements and designs, and present a toolbox of several techniques that can be used*

*to achieve the required level of privacy protection. "*

Mobile/Wireless location privacy would inevitable emerge as an important issue given the growth of that type

of communication, and the [6]obvious [7]abuses of it.

Technorati tags :

[8]Security, [9]Privacy, [10]Wireless, [11]Mobile,  
[12]Tracking

1. <http://photos1.blogger.com/blogger/1933/1779/1600/wireless5.jpg>
2. <http://en.wikipedia.org/wiki/Wardriving>
3. <http://research.microsoft.com/users/tuomaura/Publications/aura-zugenmaier-protocols04.pdf>
4. <http://research.microsoft.com/~helenw/papers/sigasia05.pdf>
5. <http://netlab.cs.ucla.edu/wiki/files/kong03mobihoc.pdf>
6. [http://news.bbc.co.uk/2/hi/programmes/click\\_online/4747142.stm](http://news.bbc.co.uk/2/hi/programmes/click_online/4747142.stm)
7. [http://www.eff.org/legal/cases/USA\\_v\\_PenRegister/](http://www.eff.org/legal/cases/USA_v_PenRegister/)
8. <http://technorati.com/tag/Security>

9. <http://technorati.com/tag/Privacy>
10. <http://technorati.com/tag/Wireless>
11. <http://technorati.com/tag/Mobile>
12. <http://technorati.com/tag/Tracking>

232

## **DVD of the Weekend - War Games (2006-03-27 14:44)**

Hi folks, as it's been a while since I last posted a quality post, I feel it's about time I catch up with some recent events.

What I'm currently working on, is gathering a very knowledgeable bunch of dudes in order to open up a discussion

on the [1]emerging market for 0day vulnerabilities, and I'm very happy about the guys that have already showed

interest in what I plan to do - more on that around the week, or the beginning of the next week.

As you're all hopefully aware by now, yet another [2]0day IE vulnerability is in the wild, so either change your

browsing habits for a little while(don't or you lose the battle, as [3]secure surfing is still possible to a certain extend), or consider switching to another alternative - security through obscurity isn't the panacea of fighting the problem

in here, instead it's just a temporary precaution. On the other hand I'm desperately trying to promote my [4]RSS

compatible feed URL to make it easier for everyone to keep up to date with posts, whereas the majority of readers

seem to enjoy reading the blog directly,

I appreciate that!

As always, it's disturbing how "quality" always becomes the excuse for security, in respect to MS delaying

patches (or is it [5]just patches [6]only?) whereas [7]WebSense is already aware of over 200 web sites disseminating

the exploit code, I wonder are they counting the hundreds of thousands of zombie pcs acting as propagation vectors.

In one of my previous posts "[8]5 things Microsoft can do to secure the Internet, and why it wouldn't?" I tried to summarize some of my thoughts on the problem, while on the other hand things definitely [9]change pretty fast as

always – for the good I hope! Was [10]the [11]participants' secrecy in place, in order not to get a "shame on you"

look from fellow hackers, whatever the reason, I doubt anyone is going to change their hats soon.

## **UPDATE :**

[12]Déjà Vu as Third Parties Ship IE Patches, and the [13]patches [14]themselves, while on the other hand it's great

that anti-virus vendors have as well started detecting malicious sites using it.

Going back this weekend's DVD (check out the previous [15]DVDs and [16]vibes as well) [17]War Games has

shaped not just imaginations back in 1983, but acted as an important factor for the rise of another generation – not

wardialers, but wannabe hackers obsessed with command'n'control strategies such as [18]Civilization 1 or [19]Dune II,

or at least that's how I remember it. Today's War Games have another dimension and it's called [20]Network-Centric

Warfare, or military communications and control over IP, and while there's a little chance an AI would malfunction

and cause Doom's day, [21]human factor mistakes will always prevail. As always, SFAM seems to have reviewed the majority of [22]cool movies, so check out the review.

Technorati tags :

[23]Weekend, [24]War Games, [25]Cyberpunk

233

1. <http://ddanchev.blogspot.com/2006/03/wheres-my-0day-please.html>
2. <http://isc.sans.org/diary.php?storyid=1223>
3. [http://www.cert.org/archive/pdf/browser\\_security0601.pdf](http://www.cert.org/archive/pdf/browser_security0601.pdf)
4. <http://feeds.feedburner.com/DanchoDanchevOnSecurityAndNewMedia>

5. <http://news.bbc.co.uk/2/hi/business/4831374.stm>
6. <http://www.internetnews.com/business/article.php/3594051>
7. <http://www.websensesecuritylabs.com/alerts/alert.php?AlertID=451>
8. <http://ddanchev.blogspot.com/2006/03/5-things-microsoft-can-do-to-secure.html>
9. <http://www.informationweek.com/windows/showArticle.jhtml?articleID=183702746>
10. <http://www.computerworld.com/securitytopics/security/story/0,10801,109606,00.html>
11. <http://www.microsoft.com/technet/security/bluehat/sessions/default.aspx>
12. <http://www.eweek.com/article2/0,1895,1943687,00.asp>
13. <http://www.eeye.com/html/research/tools/JScriptPatchSetup.exe>
14. [http://www.determina.com/security\\_center/security\\_advisories/securityadvisory\\_march272006\\_1.asp](http://www.determina.com/security_center/security_advisories/securityadvisory_march272006_1.asp)
15. <http://ddanchev.blogspot.com/2006/03/dvd-of-weekend-immortals.html>



16. <http://ddanchev.blogspot.com/2006/03/weekend-vibes-psychedelicgoa-trance.html>
17. [http://www.amazon.com/gp/product/0792838467/qid=1143463509/sr=1-1/ref=sr\\_1\\_1/104-0131442-3303906?s=dvd&v=glance&n=130](http://www.amazon.com/gp/product/0792838467/qid=1143463509/sr=1-1/ref=sr_1_1/104-0131442-3303906?s=dvd&v=glance&n=130)
18. <http://www.civfanatics.com/civ1/>
19. <http://archive.gamespy.com/legacy/halloffame/dune2.shtm>
20. [http://www.dodccrp.org/publications/pdf/Moffat\\_Complexity.pdf](http://www.dodccrp.org/publications/pdf/Moffat_Complexity.pdf)
21. [http://www.windowsecurity.com/articles/Reducing\\_Human\\_Factor\\_Mistakes.html](http://www.windowsecurity.com/articles/Reducing_Human_Factor_Mistakes.html)
22. <http://www.cyberpunkreview.com/movie/decade/1980-1989/war-games/>
23. <http://technorati.com/tag/Weekend>
24. <http://technorati.com/tag/War+Games>
25. <http://technorati.com/tag/Cyberpunk>

234

**Are cyber criminals or bureaucrats the industry's top performer? (2006-03-27 16:25)**

Last week, I came across a great article at Forbes.com, "[1]Fighting Hackers, Viruses, Bureaucracy", an excerpt :

*" Cyber security largely ends up in the backseat," says Kurtz, who prior to lobbying did stints in the State Department, the National Security Council and as an adviser to President George W. Bush on matters relating to*

*computer security. "Our job is to shine a bright light on it, to help people understand it. "*

Basically, it provides more info on how bureaucracy tends to dominate, and how security often ends up in the

"backseat". Moreover, [2]Paul Kurtz executive director of the [3]Cyber Security Industry Alliance and it's multi-billion market capitalization [4]members can indeed become biased on a certain occasions.

Still, he provides his viewpoint on important legislative priorities :

### **- setting national standards for data breach notification**

PrivacyRight's "[5]Chronology of Data Breaches Reported Since the ChoicePoint Incident" keeps growing with

the recent [6]Fidelity's loss of laptop. Standards for data breach notification are important, and the trends is growing with more states joining this legal obligation to notify customers in case their personal information is breached into

- given they are actually aware of the [7]breach. Moreover, with companies wondering "[8]To report, or not to

report?" and let me add "What is worth reporting?", Uncle Sam has a lot of work to do, that will eventually act as a benchmark for a great number of developed/developing countries. [9]Personal data security breaches are inevitable

given the unregulated ways of storing and processing the data, or is it just too many attack vectors malicious identity

thieves could take advantage of these days? E-banking is still [10]insecure, and [11]protection against phishing seems

too complicated for the "average victim". [12]Compliance means expenses as well, so it better be a long-term one, if one exists given today's challenging threatscape.

### **- a law on spyware**

Do your [13]homework and try to bring some sense into who's liable for what. [14]Claria obviously isn't, and

it's not just pocket money we're talking about here. Spyware legislations are a very interesting topic, that I also find quite contradictory, laws and legislations change quite often, but given the Internet's disperse international laws,

or the lack of such, a spyware/adware's vendor business practices may actually be legal under specific laws, or the simple absence of these.

### **- and ratification of the Council of Europe's Convention on Cybercrime**

That's important, the [15]Convention on Cybercrime I mean, would they go as far as ratifying Europe's well

known stricter compared to the U.S privacy laws? Excluding the [16]data retention legislation, and various other

235

[17]privacy issues to keep in mind, there's this tiny sentence in its [18]privacy policy " *Google processes personal information on our servers in the United States of America and in other countries.*

*In some cases, we process personal information on a server outside your own country"*, makes it so virtually easy to bypass a nation's privacy regulations that I wonder why it hasn't received the necessary attention already. On

the other hand, we have Interpol acting as a common [19]cybercrime body, that according to a [20]recent article :

*" We need an integrated legal framework to exchange data. A lot of legislation doesn't consider a data stream*

*as evidence, because the evidence is hidden behind 0s and 1s. We have to rethink the legislative framework".*

There is already such and that's the [21]NSP-SEC - a volunteer incident response mailing list, which coordi-

nates the interaction between ISPs and NSPs in near real-time and tracks exploits and compromised systems as well

as mitigates the effects of those exploits on ISP networks.

Still, The Internet Storm Center remains the most popular [22]Internet Sensor.

No matter how many [23]security policies you develop and hopefully implement, at the bottom line you ei-

ther need [24]regulations or insightful [25]security czar in charge. And while the majority of industry players

profitable provide perimeter based defenses, going through "[26]2004's Annual Report to Congress on Foreign

Economic Collection and Industrial Espionage" a decision-maker will hopefully start perceiving the problem under

a different angle. While I find [27]plain-text communications a problem, Bluecoat seems to be actively working in

exactly the [28]opposite direction. And while I find measuring the real [29]cost of Cybercrime rather hard, applying

a little bit of marginal thinking still [30]comes handy. [31]The future of privacy may indeed seem shady to some,

and while [32]data mining is definitely [33]not the answer, [34]sacrificing security for privacy shouldn't be accepted

at all. Moreover, do not take a survey's results for granted, mainly because " *There's always a self-serving aspect to anything a vendor releases,*" says Keith Crosley, director of market development with messaging security vendor Proofpoint, which does a few surveys per year" - in NetworkWorld's great article "[35]It's raining IT security surveys".

To sum up, I feel in the security world it's the malicious attacker having the time and financial motivation to

"[36]spread ambitions" that outperforms, while in the financial world, it's Symantec that is the top performer -

([37]Google Finance, [38]Yahoo! Finance) with its constant acquisitions and trendy business strategy realizing the

current shift towards convergence in the industry. Wish they could also diversify and take some market share of

[39]WetPlanet Beverage's [40]Jolt Cola drink :)

Illustration by [41]Mark Zug

**UPDATE** : This post was recently featured at LinuxSecurity.com "[42]Are cyber criminals or bureaucrats the in-236

dustury's top performer?"

Technorati tags :

[43]Security, [44]Information Security, [45]Technology, [46]Compliance, [47]Survey, [48]Bureaucracy, [49]CSIA,

[50]Cybercrime

1. [http://www.forbes.com/technology/2006/03/20/beltway-cyber-security-cx\\_ag\\_0321cyber.html](http://www.forbes.com/technology/2006/03/20/beltway-cyber-security-cx_ag_0321cyber.html)

2. [https://www.csialliance.org/aboutus/structure/bio\\_paul\\_kurtz](https://www.csialliance.org/aboutus/structure/bio_paul_kurtz)

3. <https://www.csialliance.org/>

4. <https://www.csialliance.org/membership/membershiplist/>

5. <http://www.privacyrights.org/ar/ChronDataBreaches.htm>

6. [http://www.theregister.co.uk/2006/03/24/hp\\_fidelity\\_laptop/](http://www.theregister.co.uk/2006/03/24/hp_fidelity_laptop/)

7. <http://ddanchev.blogspot.com/2006/02/detecting-intruders-and-where-to-look.html>
8. <http://ddanchev.blogspot.com/2006/01/to-report-or-not-to-report.html>
9. <http://ddanchev.blogspot.com/2006/01/personal-data-security-breaches.html>
10. <http://ddanchev.blogspot.com/2006/01/security-threats-to-consider-when.html>
11. <http://ddanchev.blogspot.com/2006/03/anti-phishing-toolbars-can-you-trust.html>
12. <http://www.theiia.org/download.cfm?file=94803>
13. <http://ddanchev.blogspot.com/2006/03/practical-complexities-of-adware.html>
14. [http://www.spamdailynews.com/publish/Claria\\_exiting\\_adware\\_business.asp](http://www.spamdailynews.com/publish/Claria_exiting_adware_business.asp)
15. <http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm>
16. <http://www.dataretentionisnosolution.com/>
17. <http://www.edri.org/>
18. <http://www.google.com/privacy.html>
19. <http://www.interpol.int/Public/TechnologyCrime/default.asp>
20. <http://news.zdnet.co.uk/0,39020330,39258540,00.htm>

21. <http://puck.nether.net/mailman/listinfo/nsp-security>
22. [http://www.usenix.org/events/sec05/tech/bethencourt/bethencourt\\_html/](http://www.usenix.org/events/sec05/tech/bethencourt/bethencourt_html/)
23. <http://www.windowsecurity.com/pages/security-policy.pdf>
24. <http://www.csoonline.com/research/compliance/index.html>
25. <http://www.securityfocus.com/columnists/394>
26. <http://ddanchev.blogspot.com/2005/12/insiders-insights-trends-and-possible.html>
27. <http://ddanchev.blogspot.com/2006/01/would-we-ever-witness-end-of-plain.html>
28. [http://www.bluecoat.com/news/releases/2006/030806\\_survey.html](http://www.bluecoat.com/news/releases/2006/030806_survey.html)
29. <http://ddanchev.blogspot.com/2006/01/why-we-cannot-measure-real-cost-of.html>
30. <http://ddanchev.blogspot.com/2006/01/fbis-2005-computer-crime-survey-whats.html>
31. <http://ddanchev.blogspot.com/2006/03/future-of-privacy-dont-over-empower.html>
32. <http://ddanchev.blogspot.com/2006/03/data-mining-terrorism-and-security.html>
33. <http://www.wired.com/news/columns/0,70357-0.html>



34. <http://ddanchev.blogspot.com/2006/03/security-vs-privacy-or-whats-left-from.html>
35. <http://www.networkworld.com/news/2006/032006-security-surveys.html>
36. <http://www.packetstormsecurity.org/papers/general/malware-trends.pdf>
37. <http://finance.google.com/finance?q=symantec>
38. <http://finance.yahoo.com/q?s=SYMC>
39. <http://www.joltcola.com/>
40. [http://en.wikipedia.org/wiki/Jolt\\_Cola](http://en.wikipedia.org/wiki/Jolt_Cola)
41. <http://www.markzug.com/>
42. <http://www.linuxsecurity.com/content/view/122136/65/>
- 237
43. <http://technorati.com/tag/Security>
44. <http://technorati.com/tag/Information+Security>
45. <http://technorati.com/tag/Technology>
46. <http://technorati.com/tag/Compliance>
47. <http://technorati.com/tag/Survey>
48. <http://technorati.com/tag/Bureaucracy>
49. <http://technorati.com/tag/CSIA>

50. <http://technorati.com/tag/Cybercrime>

238

## **Visualization in the Security and New Media world (2006-03-31 11:36)**

[1][2]Information visualization seems to be a growing trend in today's [3]knowledge driven, and information-

overloaded society. The following represents a URL tree graph of the Security Mind Streams blog – looks resourceful!

Want to freely graph your site/blog? Take advantage of [4]Texone's tree, just make sure you don't forget to press the ESC key at a certain point.

In my first post related to "[5]Visialization, intelligence and the Starlight project" I introduced you a fully realistic and feasible solution to filtering important indicators whatever the reason. Moreover, I also came across a great

[6]visualization of malware activity in another post summarizing [7]malware trends around February. What I'm truly

enjoying, is the research efforts put in the concept by both, security/IT professionals, and new media companies

realizing that the current state of the mature text-based Web.

[8]

Ever wanted to see how noisy connect() scans actually are? In early stage of its development, people are al-

ready experimenting with the idea, find more about while going through "[9]Passive Visual Fingerprinting of Network Attack Tools" paper.

Things are getting much more quantitative and in-depth in another recommended reading on the topic "[10]Real-

Time Visualization of Network Attacks on High-Speed Links" whose purpose is to " *show that malicious traffic flows such as denial-of-service attacks and various scanning activities can be visualized in an intuitive manner. A simple but novel idea of plotting a packet using its source IP address, destination IP address, and the destination port in a 3-dimensional space graphically reveals ongoing attacks. Leveraging this property, combined with the fact that only three header fields per each packet need to be examined, a fast attack detection and classification algorithm can be devised.* "

Presented at this year's BlackHat con "[11]Malware Cinema, a Picture is Worth a Thousand Packets" will pro-

vide with much more fancy visualization concepts related to malware. Originally presented by [12]Gregory Conti, you

can also download the [13]associated resources, and keep an eye on the [14]audio in case you didn't attend the con.

As far as [15]new media is concerned, I'm so impatient to witness more developments given how boring I find

any of the browsers I've used so far – and there're a lot of developments going on as always! [16]Virtual worlds have

the potential to change the face of the Web, the text/image based one the way we know it.

Remember how the federal agents were chatting face-in-face with the malicious attacker through the innova-

tive and programmed for the masses browser, in [17]NetForce? [18]Hive7 is the alternative in 2006, and if you spend

some with it, you'll be impressed by its potential – say goodbye to the good old IRC?

239

**UPDATE** : LinuxSecurity.com picked up the post "[19]Visualization in the Security and New Media world"

More resources can also be found at :

[20]CAIDA Visualization Tools

[21]NAV - Network Analysis Visualization

[22]Digital Genome Mapping - Advanced Binary Malware Analysis

[23]A Visualization Methodology for Characterization of Network Scans

[24]NVisionIP : An Interactive Network Flow Visualization Tool for Security

[25]Exploring Three-dimensional Visualization of Intrusion Detection Alerts and Network Statistics

[26]Attacking Information Visualization System Usability Overloading and Deceiving the Human

[27]Security Event Visualization and Analysis - [28]courtesy of CoreLabs

[29]A Visualization Paradigm for Network Intrusion Detection

[30]FireViz: A Personal Firewall Visualizing Tool - the

[31]FireViz project

Technorati tags:

[32]Security, [33]Information Security, [34]Monitoring,

[35]Visualization, [36]Network, [37]New Media

1.

[http://photos1.blogger.com/blogger/1933/1779/1600/security\\_mind\\_streams.jpg](http://photos1.blogger.com/blogger/1933/1779/1600/security_mind_streams.jpg)

2. [http://en.wikipedia.org/wiki/Information\\_visualization](http://en.wikipedia.org/wiki/Information_visualization)

3. [http://en.wikipedia.org/wiki/Knowledge\\_visualization](http://en.wikipedia.org/wiki/Knowledge_visualization)

4. <http://www.texone.org/tree/tree.php?id=applet>

5. <http://ddanchev.blogspot.com/2006/01/visualization-intelligence-and.html>

6. <http://www.e-things.org/worms/>

7. <http://ddanchev.blogspot.com/2006/02/recent-malware-developments.html>

8.

[http://photos1.blogger.com/blogger/1933/1779/1600/nmap\\_visualization.jpg](http://photos1.blogger.com/blogger/1933/1779/1600/nmap_visualization.jpg)

9.

[http://www.rumint.org/gregconti/publications/20040617\\_Viz\\_Sec\\_Fingerprinting.pdf](http://www.rumint.org/gregconti/publications/20040617_Viz_Sec_Fingerprinting.pdf)

10. <http://netlab.snu.ac.kr/publications/paper/radar.pdf>

11. <http://www.blackhat.com/presentations/bh-europe-06/bh-eu-06-Conti/bh-eu-06-conti.pdf>
12. <http://www.blackhat.com/html/bh-europe-06/bh-eu-06-speakers.html#Conti>
13. <http://www.blackhat.com/presentations/bh-europe-06/bh-eu-06-Conti/bh-eu-06-conti-resources.zip>
14. <http://www.blackhat.com/html/bh-media-archives/bh-archives-2006.html>
15. [http://en.wikipedia.org/wiki/New\\_media](http://en.wikipedia.org/wiki/New_media)
16. [http://en.wikipedia.org/wiki/Virtual\\_world](http://en.wikipedia.org/wiki/Virtual_world)
17. <http://www.imdb.com/title/tt0158423/>
18. <http://hive7.com/>
19. <http://www.linuxsecurity.com/content/view/122180/65/>
20. <http://www.caida.org/tools/visualization/>
21. <http://www.cs.ubc.ca/~spark343/NAV.pdf>
22. [http://www.f-secure.com/weblog/archives/carrera\\_erdelyi\\_VB2004.pdf](http://www.f-secure.com/weblog/archives/carrera_erdelyi_VB2004.pdf)
23. <http://www.cs.ucdavis.edu/~ma/papers/scanvis.pdf>
24. <http://www.projects.ncassr.org/sift/papers/smc2004.pdf>
25. <http://www.projects.ncassr.org/sift/vizsec/proceedings/2005/paper14.ppt>

26.

<http://cups.cs.cmu.edu/soups/2005/2005proceedings/p89-conti.pdf>

27.

[http://www.coresecurity.com/corelabs/projects/event\\_visualization\\_and\\_analysis.php](http://www.coresecurity.com/corelabs/projects/event_visualization_and_analysis.php)

28.

[http://www.coresecurity.com/corelabs/projects/event\\_visualization\\_and\\_analysis/CORE\\_WISDOM-UserGuide.pdf](http://www.coresecurity.com/corelabs/projects/event_visualization_and_analysis/CORE_WISDOM-UserGuide.pdf)

240

29. <http://www.cs.utah.edu/~draperg/research/IAS05.pdf>

30. <http://groups.csail.mit.edu/uid/projects/fireviz/nidhi-thesis.pdf>

31. <http://groups.csail.mit.edu/uid/projects/fireviz/>

32. <http://technorati.com/tag/Security>

33. <http://technorati.com/tag/Information+Security>

34. <http://technorati.com/tag/Monitoring>

35. <http://technorati.com/tag/Visualization>

36. <http://technorati.com/tag/Network>

37. <http://technorati.com/tag/New+Media>

241

**March's Security Streams (2006-03-31 15:13)**

A quick summary of March's Security Streams ( [1]January, [2]February ). It was an unbelievably busy month, and

while I'm multitasking and diversifying on a daily basis, I'm certain you've enjoyed this month's streams, thanks for

all the feedback you've been sending, it's a small world if you just let yourself realize it!

**1.** "[3]DVD of the (past) weekend" The Lawnmower man - God made him simple, Science made him God!

**2.** "[4]February's Security Streams" a summary of all the posts during February

**3.** "[5]Anti Phishing toolbars - can you trust them?" Recent phishing trends and the usefulness of anti-phishing toolbars discussed - at the bottom line the complexity of the relatively simple concepts seems to ruin the whole

effect, but wish phishing was that simple!

**4.** "[6]Data mining, terrorism and security" Commentary on NSA's data mining interests and the still active Total Information Awareness program. Data mining is a very popular trend towards fighting terrorism - and too

ambitious, whereas storage of someone's life in a digital form is getting even cheaper, making sense of it all in a

timely fashion still remains the biggest problem

**5.** "[7]5 things Microsoft can do to secure the Internet, and why it wouldn't?" That's the second most popular post this month, right after "[8]Where's my Oday, please?". Basically, it gives an overview of key points Microsoft can execute in order to secure the insecure by default Internet, and why it



wouldn't. The post isn't biased at all, it's just the fact that their QA procedures open up the most easily exploited windows of vulnerability ever – client side attacks

on the IE browser. As a matter of fact, Fortune's latest issue has interviewed Steve Balmer in their **QuestionAuthority** column – important fact MS's investors should keep in mind in respect to the future competitiveness of the company

is how Balmer's kids are forbidden from using iPods and Google, which is very sad

**6.** "[9]The Future of Privacy = don't over-empower the watchers!" We sacrifice our privacy, or have it abused on a daily basis in order to function in today's digital society, whereas there's nothing groundbreaking as a future

trend besides giving too much power to the Watchers ensuring our "[10]Security vs Privacy or what's left left from it"

**7.**

"[11]Where's my 0day, please?" Introducing the International Exploits Shop and providing relevant com-

ments on the current state of the market for software vulnerabilities – I wonder are the intermediaries already

talking/realizing the potential for an Ebay auction model as given the growing number of both sellers and buyers,

such a model would sooner or later emerge. If it does not, you will continue coming across or digging for sites

offering fresh 0day exploits that have the capacity to keep the media echo for yet another several weeks. CERT is

totally out of the question, end users doesn't know what is going on, and everyone is trying to cash for being a vulnerability digger, not a researcher!

## 8.

"[12]DVD of the Weekend - The Immortals" Forget entertainment and enjoy this visionary adaptation of

Enki Bilal's Nikopol Trilogy

**9.** "[13]Security vs Privacy or what's left from it" Sacrifices drive success to a certain extend, whereas Security shouldn't be sacrifices for Privacy, at any cost!

**10.** "[14]Old physical security threats still working" The old physical security trick of abusing a CD/DVD's autostart feature by installing malware on the PC seems to be fully working even today, which isn't a big suprise at all.

Physical security threats have greatly change on the other hand as employers themselves have realized the possibility

for [15]insider abuse. And while you might be a little more secure from threats like these, at the end of they day

you'll probably have your boss snooping around to find out where's that abnormal P2P traffic coming from :)

## 11.

"[16]Getting paid for getting hacked" Cyber insurance seems very attractive, and it really is, have your

company's databases stolen, you'll get premium for it, receive a DDoS extortion letter, get it paid with a smile on

the

[17]herder's face. Moreover, considering the big picture, I feel you'd rather have a security vendor take care of the

consultation process, with the idea that their revenues will be at least spend on R &D security investments compared to an insurance company, or that's how at least I see it

**12.** "[18]Successful" communication" Dilbert rocks my world, my most important point on commercializing vulnerability research is how it's happening in exactly the worst moment ever. The immature concept of reporting

vulnerabilities and the economics of the process itself didn't really need money in between. In the eyes of these

vendors, which as a matter of fact go through my posts, I am a naysayer, and I'm not. I'm just trying to keep up a

constructive discussion, and the results of it will soon be posted in here

**13.** "[19]Weekend Vibes - Psychedelic/Goa Trance" My music evolution went through Rainbow, Deep Purple,

started getting "hard" with Metallica, Off Spring, Guano Apes, to today's mix of alternative, classic rock and psychedelic/goa trance. No matter how your taste changes, don't forget where you've started from

**14.** "[20]Is a Space Warfare arms race really coming?" Yes, it is and the more awareness is build on this issue, the higher the public discussion and hopefully, transparency of the activities. I find Secrecy a double-edged sword

for an intelligence/military agency, as sometimes you just need to hear an average person's opinion on your megalomaniac ambitions. But given you are sincerely backed up by a couple of billion dollars budget, your purchasing power becomes a bad habit of yours

243

**15.** "[21]The Practical Complexities of Adware Advertising" Advertising players simply cannot periodically evaluate the [22]maliciousness of their members as they will lose the scale necessary to keep the revenues growing. The

participants on the other hand, are indeed getting ads and paid for displaying them, and of course, questionable

content from time to time. Searching around the [23]IAB's site however, you wouldn't find any info on the idea of

spyware/adware in today's booming online advertising market

**16.** "[24]Privacy issues related to mobile and wireless Internet access" Both end users and companies are "going mobile" and therefore the possibilities for privacy violations/physical security location are getting even more relevant

**17.** "[25]DVD of the Weekend - War Games" A little something on the movie and the recent "yet another Microsoft IE 0day" in the wild case

**18.** "[26]Are cyber criminals or bureaucrats the industry's top performer?" Paper tigers have an unprecedented effect

on the loss of productivity and a society's progress – the worst thing is how much they actually enjoy it! A very resourceful post that covers some important issues to keep in mind

**19.** "[27]Visualization in the Security and New Media world" or why a picture is worth a thousand packets?

**UPDATE :** Here are the unique and returning visitor graphs for the last several months, the outcome? Learn

to understand your readers and how to retain them, thank you all for expressing your comments, contacting me, and

keeping the discussion going!

Technorati tags :

[28]Security, [29]Information Security

1. <http://ddanchev.blogspot.com/2006/01/januarys-security-streams.html>
2. <http://ddanchev.blogspot.com/2006/03/februarys-security-streams.html>
3. <http://ddanchev.blogspot.com/2006/03/dvd-of-past-weekend.html>
4. <http://ddanchev.blogspot.com/2006/03/februarys-security-streams.html>
5. <http://ddanchev.blogspot.com/2006/03/anti-phishing-toolbars-can-you-trust.html>
6. <http://ddanchev.blogspot.com/2006/03/data-mining-terrorism-and-security.html>

7. <http://ddanchev.blogspot.com/2006/03/5-things-microsoft-can-do-to-secure.html>

8. <http://ddanchev.blogspot.com/2006/03/wheres-my-0day-please.html>

244

9. <http://ddanchev.blogspot.com/2006/03/future-of-privacy-dont-over-empower.html>

10. <http://ddanchev.blogspot.com/2006/03/security-vs-privacy-or-whats-left-from.html>

11. <http://ddanchev.blogspot.com/2006/03/wheres-my-0day-please.html>

12. <http://ddanchev.blogspot.com/2006/03/dvd-of-weekend-immortals.html>

13. <http://ddanchev.blogspot.com/2006/03/security-vs-privacy-or-whats-left-from.html>

14. <http://ddanchev.blogspot.com/2006/03/old-physical-security-threats-still.html>

15. <http://ddanchev.blogspot.com/2005/12/insiders-insights-trends-and-possible.html>

16. [http://ddanchev.blogspot.com/2006/03/getting-paid-for-getting-hacked\\_17.html](http://ddanchev.blogspot.com/2006/03/getting-paid-for-getting-hacked_17.html)

17. <http://ddanchev.blogspot.com/2006/01/what-are-botnet-herds-up-to.html>

18. <http://ddanchev.blogspot.com/2006/03/successful-communication.html>

19. <http://ddanchev.blogspot.com/2006/03/weekend-vibes-psychedelicgoa-trance.html>
20. <http://ddanchev.blogspot.com/2006/03/is-space-warfare-arms-race-really.html>
21. <http://ddanchev.blogspot.com/2006/03/practical-complexities-of-adware.html>
22. <http://ddanchev.blogspot.com/2006/02/look-whos-gonna-cash-for-evaluating.html>
23. <http://www.iab.net/>
24. <http://ddanchev.blogspot.com/2006/03/privacy-issues-related-to-mobile-and.html>
25. <http://ddanchev.blogspot.com/2006/03/dvd-of-weekend-war-games.html>
26. <http://ddanchev.blogspot.com/2006/03/are-cyber-criminals-or-bureaucrats.html>
27. <http://ddanchev.blogspot.com/2006/03/visualization-in-security-and-new.html>
28. <http://technorati.com/tag/Security>
29. <http://technorati.com/tag/Information+Security>

245

## **2.4**

### **April**

246

## **Wanna get yourself a portable Enigma encryption machine? (2006-04-03 13:12)**

Hurry up, you still have 5 hours to participate in the [1]sale at Ebay as the BetaNews [2]reported " *eBay has long been a purveyor of the unusual and the unique, but it's not often an authentic piece of tech history captures as much attention as the Enigma 3 portable cipher machine that has racked up bids of almost 16,000 euros. The Enigma*

*device was used extensively by Nazi Germany during World War II. "*

[3]The Enigma machine was a key success factor for the Germans during WWII, until of course its messages

started getting deciphered, it's great someone managed to preserve and resell one. Today's situation is entirely

different, namely an average Internet user can easily encrypt data achieving military standards with the use of public

tools, where [4]Phil Zimmerman's PGP has been cause troubles for governments across the world since its release.

However, what the majority of end users don't realize is the how the keys lenght and the passphrase's quality

means totally nothing when [5]law enforcement is sometimes empowered to use spyware, and that [6]quantum

cryptography is also subject to attacks. Client side attacks and social engineering ones don't take into consideration

any key lenght - just naivety. In one of my previous posts "[7]Get the chance to crack unbroken Nazi Enigma ciphers"



I mentioned about the existence of a distributed project to crack unbroken nazi ciphers you can freely partici-

pate into. Being a total paranoid in respect to my favorite SetiATHome, you should also consider the possibility of a

[8]SETI Hacker – which partly happened in [9]Contact in case you reckon.

Technorati tags :

[10]Cryptography, [11]Encryption, [12]Enigma

1.

[http://cgi.ebay.de/Enigma-3-Walzen-Chiffriermaschine-Chiper-Weltkrieg-1941\\_W0QQitemZ6265092168QQcategoryZ40820QQrdZ1QQcmdZViewItem](http://cgi.ebay.de/Enigma-3-Walzen-Chiffriermaschine-Chiper-Weltkrieg-1941_W0QQitemZ6265092168QQcategoryZ40820QQrdZ1QQcmdZViewItem)

2.

[http://www.betanews.com/article/High\\_Bids\\_for\\_WWII\\_Enigma\\_Machine/1143755592](http://www.betanews.com/article/High_Bids_for_WWII_Enigma_Machine/1143755592)

3. [http://en.wikipedia.org/wiki/Enigma\\_machine](http://en.wikipedia.org/wiki/Enigma_machine)

4. <http://www.mit.edu/~prz/EN/index.html>

5. <http://it.slashdot.org/article.pl?sid=04/12/13/1925240&tid=172&tid=17>

6. <http://ics.org.ru/pubsfiles/e/418pdf.pdf>

7. <http://ddanchev.blogspot.com/2006/02/get-chance-to-crack-unbroken-nazi.html>

8. [http://home.fnal.gov/~carrigan/SETI/SETI\\_Hacker.htm](http://home.fnal.gov/~carrigan/SETI/SETI_Hacker.htm)

9. <http://www.imdb.com/title/tt0118884/>
10. <http://technorati.com/tag/Cryptography>
11. <http://technorati.com/tag/Encryption>
12. <http://technorati.com/tag/Enigma>

247

### **The "threat" by Google Earth has just vanished in the air (2006-04-05 17:39)**

Or has it actually? In one of my previous posts "[1]Security quotes : a FSB (successor to the KGB) analyst on Google Earth" I mentioned the usefulness of [2]Google Earth by the general public, and the possibility to assist terrorists.

The most popular argument on how useless the publicly available satellite imagery is that it doesn't provide a

high-resolution images, and recent data as well – that's of course unless you don't [3]request [4]one, but isn't it

bothering you that here we have a street-side drive-by POC?

The recently introduced [5]Windows Live Local Street-Side Drive-by ([6]A9's maps have been around for quite

a while), is setting a new benchmark for interactive [7]OSINT – if any as this is also a [8]privacy violation that can be compared with efforts like [9]these if it was in real-time. Having had several conversations with a friend that's way

too much into satellite imagery than me, I've realized that starting from the basic fact of targeting a well known or

a [10]movie-plot location doesn't really requires satellite imagery. I find that today's sources basically provoke the

imagination and the self-confidence - and hopefully nothing more!

There have been [11]numerous articles on the threat posed by Google Earth, and [12]India seems to be the

most concerned country about this for the time being :

*" Chief of the Indian Army General J.J. Singh warns that Google Earth could endanger national security by providing high resolution photographs of strategic defense facilities. The software could prove especially useful to countries that do not have their own satellite capabilities. Singh called Google Earth a shared concern for all countries, requiring all countries to cooperate to address the issue. Indian President APJ Abdul Kalam has also expressed concerns over Google Earth and national security. "*

You can spend hours counting the cars in front of NSA's parking lot through public satellite imagery resources,

still you would never get to see what's going on in there, I guess things have greatly changed since the days when

tourists sent over the USSR, or exactly the opposite, to the U.S, would try to get hold of as many [13]maps as possible

finish the puzzle.

In some of my previous posts on [14]Cyberterrorism, I said that terrorists are not rocket scientists until we

make them feel so, and I'm still sticking to this statement, what about you? As a matter of fact, Schneier is inviting

everyone to participate in the [15]Movie-Plot Threat contest - stuff like [16]terrorist EMP warfare, [17]Nuclear truck

bombs (the same story from 3 [18]years ago), and other science fiction scenarios worth keeping an eye on.

Terrorism is a profitable paranoia these days, that's constantly fuelling further growth in defense and intelli-

gence spending, as satellite imagery is promoted for the bust of [19]Bin Laden, whereas their [20]infrastructure

seems to pretty safe, isn't it? (More photos, [21]1, [22]2, [23]3, [24]4, [25]5, [26]6) I'd rather we have known

parties as an adversary, the way it used to be during the [27]Cold War, whose competition [28]sent us in Space, and

[29]landed us on [30]the Moon , instead of seeing terrorists everywhere and missing the [31]big opportunity.

248

Technorati tags:

[32]Security, [33]Terrorism, [34]Cyberterrorism, [35]Privacy, [36]Google Earth, [37]Google Maps, [38]Space,

[39]Microsoft Live, [40]New Media

1. <http://ddanchev.blogspot.com/2006/01/security-quotes-fsb-successor-to-kgb.html>

2. <http://earth.google.com/>

3. <http://www.geoeye.com/>
4. <http://www.digitalglobe.com/>
5. <http://preview.local.live.com/>
6. <http://maps.a9.com/>
7. <http://en.wikipedia.org/wiki/OSINT>
8. <http://ddanchev.blogspot.com/2006/03/security-vs-privacy-or-whats-left-from.html>
9. [http://www.theregister.co.uk/2006/01/17/ic\\_eyes\\_shoreditch\\_cctv/](http://www.theregister.co.uk/2006/01/17/ic_eyes_shoreditch_cctv/)
10. <http://www.maddogproductions.com/plotomatic.htm>
11. <http://www.nytimes.com/2005/12/20/technology/20image.html?ei=5090&en=fc8a8529ca004e0c&ex=1292734800&partner=rssuserland&emc=rss&pagewanted=print>
12. <http://www.ciol.com/content/news/2006/106040308.asp>
13. [http://www.cia.gov/csi/kent\\_csi/pdf/v40i5a13p.pdf](http://www.cia.gov/csi/kent_csi/pdf/v40i5a13p.pdf)
14. <http://ddanchev.blogspot.com/2005/12/cyberterrorism-dont-stereotype-and-its.html>
15. [http://www.schneier.com/blog/archives/2006/04/announcing\\_movi.html](http://www.schneier.com/blog/archives/2006/04/announcing_movi.html)

16. <http://ddanchev.blogspot.com/2006/02/who-needs-nuclear-weapons-anymore.html>
17. <http://www.newsmax.com/archives/ic/2005/12/19/141516.shtml>
18. <http://www.foxnews.com/story/0,2933,76873,00.html>
19. <http://www.usatoday.com/tech/news/2001/10/5/attack-space-search.htm>
20. <http://www.time.com/time/2001/underthreat/caves/index.html>
21. <http://www.transglobal-aerospace.co.uk/Afganistan/caves1.jpg>
22. <http://www.transglobal-aerospace.co.uk/Afganistan/caves2.jpg>
23. <http://www.telegraph.co.uk/news/graphics/2001/11/29/whunt229big.jpeg>
24. <http://www.defendamerica.mil/images/photos/pi021302a2.jpg>
25. <http://www.benthere.com/Afghan/25DEC/caves.jpg>
26. <http://www.pritchettcartoons.com/cartoons/cave.gif>
27. [http://en.wikipedia.org/wiki/Cold\\_War](http://en.wikipedia.org/wiki/Cold_War)
28. [http://en.wikipedia.org/wiki/Yuri\\_Gagarin](http://en.wikipedia.org/wiki/Yuri_Gagarin)

29. <http://history.nasa.gov/ap11ann/introduction.htm>
30. <http://moon.google.com/>
31. <http://www.google.com/mars/>
32. <http://technorati.com/tag/Security>
33. <http://technorati.com/tag/Terrorism>
34. <http://technorati.com/tag/Cyberterrorism>
35. <http://technorati.com/tag/Privacy>
36. <http://technorati.com/tag/Google+Earth>
37. <http://technorati.com/tag/Google+Maps>
38. <http://technorati.com/tag/Space>
39. <http://technorati.com/tag/Microsoft+Live>
40. <http://technorati.com/tag/New+Media>

249

### **Insider fined \$870 (2006-04-05 18:22)**

[1]Insiders still remain an [2]unresolved issue, where the biggest trade-off is the loss of productivity and trust in the organizational culture. According to the Sydney Morning Herald :

*" A court in Guangzhou, capital of the southern Chinese province of Guangdong, has upheld a lower court's*

*guilty verdict against Yan Yifan for selling stolen passwords and virtual goods related to the online game "Da Xihua Xiyou. The court upheld a \$870 US fine, arguing that victimized players had spent time, energy, and money to obtain*

*the digital items Yan sold. Yan stole the players' information while an employee for NetEase.com, the company behind the game. "*

So, it's not just [3]0days, [4]Ebay/PayPal accounts, and [5]spyware market entry positions for sale - but [6]virtual world goods as well.

While it's not a [7]top espionage [8]case, or one compared to the [9]recent arrest of " *two men, identified as*

*Lee and Chang, on charges of industrial espionage for downloading advanced mobile phone designs from employer*

*Samsung for sale to a major telecommunications firm in Kazakhstan",* insiders still represent a growing trend that according to the most recent [10]FBI's 2005 Computer Crime Survey, cost businesses **\$6,856,450**.

Then again, failing to [11]adequately quantify the costs may either fail to assess the situation, or twist the re-

sults based on unmaterialized, but expected sales, as according to the company, " *Samsung could have suffered losses of \$1.3 billion US had the sale been completed. "* Trust is vital, and so is the confidence in Samsung's business case.



Technorati tags:

[12]Security, [13]Insider, [14]Espionage

1. <http://ddanchev.blogspot.com/2005/12/insiders-insights-trends-and-possible.html>
2. <http://www.smh.com.au/news/breaking/verdict-on-virtual-property-thief-upheld/2006/04/04/1143916492279.html>
3. <http://ddanchev.blogspot.com/2006/03/wheres-my-0day-please.html>
4. <http://sunbeltblog.blogspot.com/2006/03/seen-in-wild-ebay-accounts-for-sale.html>
5. <http://www.sophos.com/pressoffice/news/articles/2006/03/russianspykits.html>
6. <http://www.msnbc.msn.com/id/6870901/>
7. <http://ddanchev.blogspot.com/2006/02/top-level-espionage-case-in-greece.html>
8. [http://www.schneier.com/blog/archives/2006/03/more\\_on\\_greek\\_w.html](http://www.schneier.com/blog/archives/2006/03/more_on_greek_w.html)
9. <http://english.chosun.com/w21data/html/news/200603/200603220030.html>
10. <http://ddanchev.blogspot.com/2006/01/fbis-2005-computer-crime-survey-whats.html>
11. <http://ddanchev.blogspot.com/2006/01/why-we-cannot-measure-real-cost-of.html>

12. <http://technorati.com/tag/Security>
13. <http://technorati.com/tag/Insider>
14. <http://technorati.com/tag/Espionage>

250

### **Securing political investments through censorship (2006-04-05 18:59)**

[1]I try to extensively blog on various [2]privacy and [3]Internet censorship related issues affecting different parts of the world, or provide comments on the big picture they way I see it.

Spending millions – [4]6 million euro here, and I guess you also wouldn't let someone spread the word whether the

cover is fancy enough for a vote or not – on [5]political campaigns to directly or indirectly influence the outcome of

an election, is a common practice these days. Whereas, trying to build a wall around a government's practices is like

having a tidal wave of comments smashing it. I recently came across the following [6]article :

*" Singapore has reminded its citizens that web users who post commentary on upcoming elections could face*

*prosecution. Election commentary is tightly controlled under Singaporean law; independent bloggers may comment*

*on the election, but must register their site with the Media Development Authority (MDA). "*

I'm so not into politics – and try not to – but threatening with prosecution on commentary, registering users,

while not first "introducing yourself" as " *During the November 2001 elections, Singapore's political parties limited their use of the Internet to posting schedules and candidate backgrounds.* " isn't the smartest long-term political strategy ever, don't you think?

More resources on the state of censorship in Singapore worth checking out are :

[7]

[8]Internet Filtering in Singapore in 2004- 2005: A Country Study

[9]EFF "Censorship - Singapore" Archive

[10]Censorship in Singapore

[11]To Net or Not to Net: Singapore's Regulation of the Internet

[12]Censorship Review Committee 2002/2003

[13]The Internet and Political Control in Singapore

Technorati tags:

[14]Censorship, [15]Politics

1.

<http://photos1.blogger.com/blogger/1933/1779/1600/tvlies.0.jpg>

2. <http://ddanchev.blogspot.com/2006/03/future-of-privacy-dont-over-empower.html>

3. <http://ddanchev.blogspot.com/2006/02/chinese-internet-censorship-efforts.html>
  4. <http://www.timesonline.co.uk/article/0,,13509-2100904,00.html>
  5. [http://en.wikipedia.org/wiki/Campaign\\_finance](http://en.wikipedia.org/wiki/Campaign_finance)
  6. <http://networks.silicon.com/webwatch/0,39024667,39157814,00.htm>
  7. [http://en.wikipedia.org/wiki/Censorship\\_in\\_Singapore](http://en.wikipedia.org/wiki/Censorship_in_Singapore)
  8. [http://www.opennetinitiative.net/studies/singapore/ONI\\_Country\\_Study\\_Singapore.pdf](http://www.opennetinitiative.net/studies/singapore/ONI_Country_Study_Singapore.pdf)
  9. <http://www.eff.org/Global/Singapore/Censorship>
- 251
10. [http://en.wikipedia.org/wiki/Censorship\\_in\\_Singapore](http://en.wikipedia.org/wiki/Censorship_in_Singapore)
  11. <http://www.law.indiana.edu/fclj/pubs/v51/no2/hoganmac.PDF>
  12. [http://www.mda.gov.sg/wms.file/mobj/mobj.316.Censorship\\_Review\\_2003.pdf](http://www.mda.gov.sg/wms.file/mobj/mobj.316.Censorship_Review_2003.pdf)
  13. <http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN002726.pdf>
  14. <http://technorati.com/tag/Censorship>

15. <http://technorati.com/tag/Politics>

252

### **Heading in the opposite direction (2006-04-05 19:51)**

Just one day before [1]April 1st 2006 I came across this [2]article :

*" German retail banker Postbank will begin using electronic signatures on e-mails to its customers to help protect them from phishing attacks. "*

Catching up with the phishers seems to be a very worrisome future strategy. Electronic Signatures by them-

selves are rarely checked by anyone, and many more attack vectors are making the idea of this totally irrelevant.

Moreover, a great research "[3]Why phishing works" was recently released and it basically outlines basic facts such as how end users doesn't pay attention to security checks, if there's a definition of such given the attack vectors

phishers have started using recently. In some of my previous posts "[4]Security threats to consider when doing

E-Banking", and "[5]Anti Phishing toolbars - can you trust them?" I mentioned many other problems related to this bigger than it seems problem, what you should also keep an eye on is the [6]good old ATM scam I hope you are

aware of.

Postbank is [7]often targeted by phishers, still, the best protection is the level of [8]security awareness stated

in here :

*" Phishing attacks have led 80 % of Germans to distrust banking related e-mails, according to TNS Infratest. "*

*Moreover, " Postbank's electronic signature service isn't possible with web-based e-mail services provided by local Internet service providers such as GMX GmbH and Freenet.de AG, according to Ebert. One exception is Web.de"*

Thankfully, but that's when you are going in exactly the opposite direction than your customers are, while try-

ing to establish reputable bank2customer relationship over email. Listen your customers first, and follow the trends,

and do not try to use the most popular dissemination vector as a future communication one.

Something else in respect to recent phishing statistics is the key summary points of the recently released,

[9]AntiPhishingGroup's Report for January, 2006 report :

- Number of unique phishing reports received in January: 17,877*
- Number of unique phishing sites received in January: 9715*
- Number of brands hijacked by phishing campaigns in January: 101*
- Number of brands comprising the top 80 % of phishing campaigns in January: 6*
- Country hosting the most phishing websites in January: United States*

- *Contain some form of target name in URL: 45 %*

253

- *No hostname just IP address: 30 %*
- *Percentage of sites not using port 80: 8 %*
- *Average time online for site: 5.0 days*
- *Longest time online for site: 31 days*

I feel there's a lot more to expect than trying to re-establish the communication over a broken channel, as far

as E-banking is concerned.

More resources you might be interested in taking a look at are :

[10]Vulnerability of First-Generation Digital Certificates and Potential for Phishing Attacks

[11]Netcraft: More than 450 Phishing Attacks Used SSL in 2005

[12]SSL's Credibility as Phishing Defense Is Tested

[13]Rootkit Pharming

[14]The future of Phishing

[15]Something is Phishy here...

[16]Phishing Site Using Valid SSL Certificates

[17]Thoughts on Using SSL/TLS Certificates as the Solution to Phishing

Technotati tags:

[18]Security, [19]Phishing, [20]Scam, [21]Banking

1. [http://en.wikipedia.org/wiki/April\\_1,\\_2006](http://en.wikipedia.org/wiki/April_1,_2006)
2. <http://www.techworld.com/security/news/index.cfm?NewsID=5686>
3. [http://people.deas.harvard.edu/~rachna/papers/why\\_phishing\\_works.pdf](http://people.deas.harvard.edu/~rachna/papers/why_phishing_works.pdf)
4. <http://ddanchev.blogspot.com/2006/01/security-threats-to-consider-when.html>
5. <http://ddanchev.blogspot.com/2006/03/anti-phishing-toolbars-can-you-trust.html>
6. <http://www.ebankingsecurity.com/article3.asp>
7. [http://www.fraudwatchinternational.com/phishing/company\\_details.php?ref\\_no=155](http://www.fraudwatchinternational.com/phishing/company_details.php?ref_no=155)
8. <http://ddanchev.blogspot.com/2006/02/security-awareness-posters.html>
9. [http://www.antiphishing.org/reports/apwg\\_report\\_jan\\_2006.pdf](http://www.antiphishing.org/reports/apwg_report_jan_2006.pdf)
10. [http://www.geotrust.com/resources/white\\_papers/pdfs/SSLVuInerabilityWPcds.pdf](http://www.geotrust.com/resources/white_papers/pdfs/SSLVuInerabilityWPcds.pdf)
11. [http://news.netcraft.com/archives/2005/12/28/more\\_than\\_4](http://news.netcraft.com/archives/2005/12/28/more_than_4)



[50\\_phishing\\_attacks\\_used\\_ssl\\_in\\_2005.html](#)

12.

[http://news.netcraft.com/archives/2004/03/08/ssls\\_credibility\\_as\\_phishing\\_defense\\_is\\_tested.html](http://news.netcraft.com/archives/2004/03/08/ssls_credibility_as_phishing_defense_is_tested.html)

13. <http://www.f-secure.com/weblog/archives/archive-022006.html#00000821>

14.

<http://www.cryptomathic.com/pdf/The%20Future%20of%20Phishing.pdf>

15. <http://www.wizardsofttechnology.com/?q=node/view/107>

16.

[http://blog.washingtonpost.com/securityfix/2006/02/the\\_new\\_face\\_of\\_phishing\\_1.html](http://blog.washingtonpost.com/securityfix/2006/02/the_new_face_of_phishing_1.html)

17. <http://hsivonen.iki.fi/phishing-certs/>

18. <http://technorati.com/tag/Security>

19. <http://technorati.com/tag/Phishing>

20. <http://technorati.com/tag/Scam>

21. <http://technorati.com/tag/Banking>

254

### **"IM me" a strike order (2006-04-12 12:35)**

[1]In my previous post "[2]What's the potential of the IM security market? Symantec thinks big" I commented on various IM market security trends, namely [3]Symantec's acquisition of IMLogic. It's also worth mentioning how a

market leader security vendor was able to quickly capitalize on the growing IM market, and turn the acquisition into

a valuable solution on the giant's [4]portfolio of solutions. What's also worth mentioning is the military interest in

instant communications in today's [5]network centric warfare powered battlefield. Today I across an interesting

[6]recent development, namely that :

*" The US Army, Navy, and Air Force have deployed protected interoperable instant messaging (IM) systems among the threebranches. Army Knowledge Online, Navy Knowledge Online, and theAir Force's Knowledge Management Portal*

*built the IM systems for 3.5 million users from Bantu's Inter-domain Messaging (IDM)gateway, a policy-driven with*

*role-based access controls. The system will carry messages over sensitive and secret networks, and can populate a*

*user's contact list with appropriate officials in the chain of command. Intelligence agencies will hook into the system to work with the military, and the Department of Homeland Security is also interested in the IM system. "*

[7]

[8]Flexible military communications have always been of great importance, and flexibility here stands for se-

curely communicating over insecure channels – IP based communications. While you might have not heard of

[9]Bantu before, to me their [10]real-time network for interagency communication sounds more like a security

through obscurity approach – temporary gain and possible long term disaster.

Could the instant communication finally solve the Intelligence Community's [11]information sharing troubles?

In a relatively [12]recent report I came across, " *a survey was hosted on the Secret Internet Protocol Router*

*Network ([13] SIPRNET) so that personnel could respond to the survey from the convenience and privacy of their own workstations.* " in order to measure the communication requirements of various staff members, some of the findings worth mentioning :

[14]MS Chat was used by at least 50 % of all command groups

- *100 % of Afloat Staffs, 86 % of Carriers, 78 % of Cruisers & Destroyers, 50 % of Support*

[15]XIRCON was used by 28 % - 50 % of command groups

- *50 % of Support, 41 % of Carriers, 32 % of Cruisers & Destroyers, 28 % of Afloat Staffs*

[16]Lotus Sametime was used by 0 – 44 % of command groups

- *44 % of Afloat Staffs, 16 % of Cruisers & Destroyers, 10 % of Carriers, 0 % of Support*

[17]mIRC was used by 13 – 33 % of command groups

- *33 % of Support, 23 % of Carriers, 22 % of Cruisers & Destroyers, 13 % of Afloat Staffs*

Lotus Sametime and mIRC seem to be only survivors, still the implications of using the above in respect to the

powerful execution of various network centric warfare events, would definitely raise not just my eyebrows for

sure. [18]Two years ago, led by IMLogic a consortium on IM threats was established, the [19]IM Threat Center, an

255

indispensable early warning system for anything related to IM malware.

Would age-old IM threats re-introduce themselves on military networks like never before? Whatever the out-

come, information overload wouldn't necessarily be solved through instant communications, but in a combination

with powerful [20]visualization [21]concepts as well.

The post recently appeared at LinuxSecurity.com "[22]IM me" a strike order"

Technorati tags:

[23]Security, [24]Military, [25]IM, [26]Technology, [27]Symantec, [28]Bantu

1.

<http://photos1.blogger.com/blogger/1933/1779/1600/strike.jpg>

2. <http://ddanchev.blogspot.com/2006/01/whats-potential-of-im-security-market.html>

3. [http://www.symantec.com/about/news/release/article.jsp?prid=20060103\\_01](http://www.symantec.com/about/news/release/article.jsp?prid=20060103_01)
4. <http://www.networkworld.com/news/2006/041006-symantec-im-security.html>
5. [http://en.wikipedia.org/wiki/Network-centric\\_warfare](http://en.wikipedia.org/wiki/Network-centric_warfare)
6. <http://www.fcw.com/article94020-04-10-06-Web>
7. [http://photos1.blogger.com/blogger/1933/1779/1600/real\\_time\\_chat1.jpg](http://photos1.blogger.com/blogger/1933/1779/1600/real_time_chat1.jpg)
8. <http://www.wired.com/wired/archive/10.02/mustread.html?pg=7>
9. <http://www.bantu.com/releases/2006.04.10.idm.php>
10. <http://www.bantu.com/products/IDMFactSheet.pdf>
11. [http://www.govexec.com/story\\_page.cfm?articleid=33191&dcn=todaysnews](http://www.govexec.com/story_page.cfm?articleid=33191&dcn=todaysnews)
12. [http://www.dodccrp.org/events/2004/CCRTS\\_San\\_Diego/CD/papers/086.pdf](http://www.dodccrp.org/events/2004/CCRTS_San_Diego/CD/papers/086.pdf)
13. <http://www.fas.org/irp/program/disseminate/siprnet.htm>
14. <http://chat.msn.com/>
15. <http://www.xircon.com/>
16. <http://www.lotus.com/products/lotussametime.nsf/wdocs/homepage>

17. <http://www.mirc.com/>
18. [http://news.com.com/Consortium+forms+IM+threat+center/2100-7355\\_3-5481414.html](http://news.com.com/Consortium+forms+IM+threat+center/2100-7355_3-5481414.html)
19. [http://www.imlogic.com/im\\_threat\\_center/index.asp](http://www.imlogic.com/im_threat_center/index.asp)
20. <http://ddanchev.blogspot.com/2006/01/visualization-intelligence-and.html>
21. <http://ddanchev.blogspot.com/2006/03/visualization-in-security-and-new.html>
22. <http://www.linuxsecurity.com/content/view/122350/2/>
23. <http://technorati.com/tag/Security>
24. <http://technorati.com/tag/Military>
25. <http://technorati.com/tag/IM>
26. <http://technorati.com/tag/Technology>
27. <http://technorati.com/tag/Symantec>
28. <http://technorati.com/tag/Bantu>

256

### **Catching up on how to lawfully intercept in the digital era (2006-04-12 19:17)**

In one of my previous posts "[1]A top level espionage case in Greece" I blogged about two cases of unlawful

interception – good old espionage practices in modern environment. What's also worth mentioning is the rush

for [2]lawful interception in the post 9/11 world, that is [3]free spirits get detained for singing or being [4]nerds,

activities you can hardly [5]datamine at the bottom line, and then again, [6]so what?

Last month, Australia extended its phone-tap laws to e-mails and SMS, OMG, [7]good morning Vietnam. An

excerpt from the [8]news item :

*" Australia has passed new laws that would allow police to intercept phone calls, e-mails, and text messages of people who are just suspected of a crime. Attorney-General Philip Ruddock says the new laws account for challenges*

*posed by technology; in December 2005, Middle Eastern and white supremacist youth used SMS messages to*

*coordinate during race riots. However, civil liberties groups warn that the laws could allow police to target the*

*privileged conversations of lawyers and journalists or to target innocent people for investigation. Australia has been tightening security laws since the September 11, 2001, terrorist attacks in the US. "*

Whether compliance, or new [9]revenue sources from a telecom/network giant's point of view, [10]lawful in-

terception has always been happening. A [11]single [12]vendor's [13]box can [14]easily [15]monitor over 30,000 DSL

connections, and while the problem still remains processing power and [16]decentralized/encrypted [17]communi-

cations, [18]steganography as a concept has always been the biggest downside of any approach from my point of view.

At the bottom line it would eventually provide the [19]ECHELON's community with more information to take

hold of, whereas retaining or trying to data mine it still remains an abstract concept whose only justification has been the contradictive [20]Able Danger scenario. It is my opinion that erasing terrabytes of intelligence information on a

terrorist group is a pure science-fiction scenario, they way there's a desperate need for a clear [21]ROI in respect to

CCTV cameras.

Don't [22]over-empower the watchers for [23]the sake of your Security, or you'll end up with a false feeling

of it.

More resources on surveillance and lawful interception worth going through are :

[24]International Campaign Against Mass Surveillance

[25]Development of surveillance technology and risk of abuse of economic information

[26]Legal Analysis of the NSA Domestic Surveillance Program

[27]Wiretapping, FISA, and the NSA



[28]Can the government track your cell phone's location without probable cause?

257

[29]Attack Detection Methods for All-Optical Networks

[30]2006 = 1984?

[31]Privacy issues related to mobile and wireless Internet access

[32]Lawful Interception of the Internet

[33]Using MAC Addresses in the Lawful Interception of IP Traffic

[34]Open Source Intelligence (OSINT)

[35]Making Intelligence Accountable: Legal Standards and Best Practice for Oversight of Intelligence Agencies

[36]What is Project ECHELON?

[37]Surveillance and Society Journal

[38]Cybercrime in New Network Ecosystem: vulnerabilities and new forensic capabilities

[39]Strategies for Lawful Intercept

[40]Summary - Lawful Interception plugtest

[41]Whistle-Blower Outs NSA Spy Room

Technorati tags:

[42]Security, [43]Intelligence, [44]Surveillance,  
[45]Wiretapping, [46]Privacy, [47]Lawful Interception

1. <http://ddanchev.blogspot.com/2006/02/top-level-espionage-case-in-greece.html>
2. [http://en.wikipedia.org/wiki/Lawful\\_interception](http://en.wikipedia.org/wiki/Lawful_interception)
3. <http://www.entertainmentwise.com/news?id=15537>
4. <http://www.guardian.co.uk/attackonlondon/story/0,16132,1575532,00.html>
5. <http://ddanchev.blogspot.com/2006/03/data-mining-terrorism-and-security.html>
6. <http://www.dataretentionisnosolution.com/>
7. <http://www.imdb.com/title/tt0093105/>
8. [http://in.today.reuters.com/news/newsArticle.aspx?type=technologyNews&storyID=2006-03-31T121038Z\\_01\\_NOOTR\\_RTRJONC\\_0\\_India-243066-1.xml](http://in.today.reuters.com/news/newsArticle.aspx?type=technologyNews&storyID=2006-03-31T121038Z_01_NOOTR_RTRJONC_0_India-243066-1.xml)
9. [http://www.theregister.co.uk/2006/02/13/ss8\\_expansion\\_3gsm/](http://www.theregister.co.uk/2006/02/13/ss8_expansion_3gsm/)
10. <http://www.blackhat.com/presentations/bh-usa-03/bh-us-03-baloo.pdf>
11. <http://www.narus.com/products/intercept.html>

12. [http://www.ss8.com/pdf/files/SS8\\_Xcipio\\_trifold.pdf](http://www.ss8.com/pdf/files/SS8_Xcipio_trifold.pdf)
13. [http://www.cisco.com/en/US/products/hw/cable/ps2217/products\\_feature\\_guide\\_chapter09186a008019b571.html](http://www.cisco.com/en/US/products/hw/cable/ps2217/products_feature_guide_chapter09186a008019b571.html)
14. <http://www.mantech.com/solutions/secureSystems.asp>
15. <http://www.dailykos.com/storyonly/2006/4/8/14724/28476>
16. <http://govexec.com/dailyfed/0406/041006nj2.htm>
17. <http://ddanchev.blogspot.com/2006/01/would-we-ever-witness-end-of-plain.html>
18. [http://www.simson.net/ref/2005/csci\\_e-170/p1/grand.pdf](http://www.simson.net/ref/2005/csci_e-170/p1/grand.pdf)
19. <http://en.wikipedia.org/wiki/ECHELON>
20. [http://en.wikipedia.org/wiki/Able\\_Danger](http://en.wikipedia.org/wiki/Able_Danger)
21. [http://www.csoononline.com/read/090105/roi\\_3826.html](http://www.csoononline.com/read/090105/roi_3826.html)
22. <http://ddanchev.blogspot.com/2006/03/future-of-privacy-dont-over-empower.html>
23. <http://ddanchev.blogspot.com/2006/03/security-vs-privacy-or-whats-left-from.html>
24. <http://www.statewatch.org/news/2005/apr/icams-report.pdf>
25. <http://www.fas.org/irp/program/process/docs/98-14-01-2en.pdf>
26. <http://volokh.com/posts/1135029722.shtml>

27. <http://www.securityfocus.com/columnists/379>
28. [http://www.eff.org/legal/cases/USA\\_v\\_PenRegister/](http://www.eff.org/legal/cases/USA_v_PenRegister/)
29. <http://www.isoc.org/isoc/conferences/ndss/98/medard.pdf>
30. <http://ddanchev.blogspot.com/2006/01/2006-1984.html>
- 258
31. <http://ddanchev.blogspot.com/2006/03/privacy-issues-related-to-mobile-and.html>
32. <http://caia.swin.edu.au/reports/030606A/CAIA-TR-030606A.pdf>
33. <http://caia.swin.edu.au/pubs/ATNAC04/branch-pavlicic-armitage-ATNAC2004.pdf>
34. [http://www.cia.gov/csi/studies/Vol49no2/reexamining\\_the\\_distinction\\_3.htm](http://www.cia.gov/csi/studies/Vol49no2/reexamining_the_distinction_3.htm)
35. [http://www.dcaf.ch/handbook\\_intelligence/\\_publications.cfm](http://www.dcaf.ch/handbook_intelligence/_publications.cfm)
36. <http://www.nsawatch.org/echelonfaq.html>
37. <http://www.surveillance-and-society.org/>
38. [http://islandia.law.yale.edu/isp/digital%20cops/papers/rutkowski\\_newcrimescene1.pdf](http://islandia.law.yale.edu/isp/digital%20cops/papers/rutkowski_newcrimescene1.pdf)
39. [http://www.nomadix.com/Files/Downloads/Applications/Strategies\\_for\\_Lawful\\_Intercept.pdf](http://www.nomadix.com/Files/Downloads/Applications/Strategies_for_Lawful_Intercept.pdf)

40.

[http://www.etsi.org/Plugtests/History/DOC/2006\\_LI\\_Report.pdf](http://www.etsi.org/Plugtests/History/DOC/2006_LI_Report.pdf)

41. <http://www.wired.com/news/technology/0,70619-0.html?tw=rss.index>

42. <http://technorati.com/tag/Security>

43. <http://technorati.com/tag/Intelligence>

44. <http://technorati.com/tag/Surveillance>

45. <http://technorati.com/tag/Wiretapping>

46. <http://technorati.com/tag/Privacy>

47. <http://technorati.com/tag/Lawful+Interception>

259

### **On the Insecurities of the Internet (2006-04-13 12:04)**

Among the most popular [1]stereotypes related to Cyberterrorism, is that of terrorists [2]shutting down the Internet,

or to put it in another way, denying access to the desperse and decentralized Internet infrastructure by attacking the

[3]Internet's root servers the way it happened back in [4]2002 – knowing Slashdot's IP in such a situation will come

as a handy nerd's habit for sure. Outages like these would eventually result in a [5]butterfly effect, such as direct

monetary losses and confidence in the today's E-commerce world.

In my previous "[6]How to secure the Internet" I commented on the [7]U.S's National Strategy to Security Cy-

berspace, moreover, I pointed out some issues to consider in respect to the [8]monoculture that's affecting the

entire population. While today's threatscape is constantly changing, it still points out key points points such as :

### **- Improve the Security and Resilience of Key Internet Protocols**

*" The Internet is currently based on Internet Protocol version 4 (IPv4). Some organizations and countries are moving to an updated version of the protocol, version 6 (IPv6). IPv6 offers several advantages over IPv4. In addition to offering a vast amount of addresses, it provides for improved security features, including attribution and native IP security (IPSEC), as well as enabling new applications and capabilities. Some countries are moving aggressively to adopt IPv6.*

*Japan has committed to a fully IPv6 based infrastructure by 2005. The European Union has initiated steps to move to*

*IPv6. China is also considering early adoption of the protocol. "*

In my previous "[9]The current state of IP Spoofing" post, I mentioned that if you can spoof there's no accou-

tability, and you can even get DDoSed by gary7.nsa.gov. But until then we would have to live with the current

situation, or keep building awareness on the issue of course.

## **- Secure the Domain Name System**

*" DNS serves as the central database that helps route information throughout the Internet. The ability to route information can be disrupted when the databases cannot be accessed or updated or when they have been corrupted.*

*Attackers can disrupt the DNS by flooding the system with information or requests or by gaining access to the system and corrupting or destroying the information that it contains. "*

During March, Randal Vaughn and Gadi Evron released a practical study entitled "[10]DNS Amplification At-

tacks" pointing out that :

*" Our study is based on packet captures and logs from attacks reported to have a volume of 2.8Gbps.*

*We*

*study this data in order to further understand the basics of the reported recursive name server amplification attacks which are also known as DNS amplification or DNS reflector attacks. One of the networks under attack, Sharktech,*

*indicated some attacks have reached as high as 10Gbps and used as many as 140,000 exploited name servers. In*

*addition to the increase in the response packet size, the large UDP packets create IP protocol fragments. Several*

260

*other responses also contribute to the overall effectiveness of these attacks. "*

It feels like a deja vu moment compared to Mixer's release of his award-winning "[11]Protecting against the

unknown" research and the emergence of DDoS attacks(read the [12]complete story, and keep in mind that it's

wasn't [13]iDefense, but [14]PacketStormSecurity offering \$10k rewards back in 2000). VeriSign indeed detailed

[15]massive denial-of service attack, and [16]Slashdot also picked up the story. Most importantly, the event also

attracted the [17]U.S government's attention, but what you should also keep in mind is that :

*" In order to create an 8Gbps attack using carefully crafted zones, you need no more than 200 home PCs on ba-*

*sic DSL lines," Joffe said. That math assumes about 200 bots eating up a full 512Kbps connection with lots of 60-byte DNS queries, each of which is amplified 70x into a 4,200-byte reply against the attacker's target. To put that in*

*perspective, Russian hacking crews advertise that they will place the malware of your choice on 1,000 bots for a mere \$25, according to the Internet Storm Center. "*

No [18]0day necessary, but [19]DDoS on demand/hire, [20]and [21]renting [22]botnets are the practices worth

mentioning the way I pointed them out in my [23]Future trends of malware research.

## **-Border Gateway Protocol**

*" Of the many routing protocols in use within the Internet, the Border Gateway Protocol (BGP) is at greatest risk of*



*being the target of attacks designed to disrupt or degrade service on a large scale. BGP is used to interconnect the thousands of networks that make up the Internet. It allows routing information to be exchanged between networks*

*that may have separate administrators, administrative policies, or protocols. "*

Interdomain routing communications are like empowering assembly line workers with the ability to stop the

line at anytime, or have a claim on it, a tricky option sometimes. A recently released research(2005) "[24]A Survey of BGP Security" points out the bottom line these days :

*" We centrally note that no current solution has yet found an adequate balance between comprehensive secu-*

*urity and deployment cost. "* Still, [25]IETF's Routing Protocol Security Requirements (rpsec) are worth the read.

What I truly hope, is that any of these guidelines wouldn't end up on a [26]paper tiger's desk for years to

come, namely they would eventually get implemented and Internet2 would end up dealing with a more advanced

set of security problems compared to the [27]current [28]ones.

My point is that, while only the [29]paranoid [30]survive, seeing [31]ghosts here and there is like totally miss-

ing the big picture – Richard Clarke for instance once [32]said that " *If there's a major devastating cyberspace security attack, the Congress will slam regulation on the industry faster than anything you can imagine. So, it's in the industry's best interest to get the job done right before something happens.* " But when, and how it would affect the commercial side of the question, that is how visionary are the vendors themselves to anticipate the future in here?

No one would want to shut down the Internet as terrorists are actively using it for propaganda, communica-

tion, and open source intelligence. Still, the [33]deceptive PSYOPS initiated by terrorist sympathizers or [34]wannabe

such is what will continue to hit the deadlines – just don't miss the big picture!

**UPDATE :** The post just appeared at LinuxSecurity.com "[35]On the Insecurities of the Internet"

Technorati tags:

[36]Security, [37]Information Security, [38]Internet, [39]Internet2, [40]DDoS, [41]Networking, [42]IPv6, [43]VeriSign

1. <http://ddanchev.blogspot.com/2005/12/cyberterrorism-dont-stereotype-and-its.html>
2. <http://www.turnofftheinternet.com/>
3. [http://en.wikipedia.org/wiki/Root\\_nameserver](http://en.wikipedia.org/wiki/Root_nameserver)
4. <http://d.root-servers.org/october21.txt>
5. <http://www.imdb.com/title/tt0289879/>

6. <http://ddanchev.blogspot.com/2006/01/how-to-secure-internet.html>
7. [http://www.whitehouse.gov/pcipb/cyberspace\\_strategy.pdf](http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf)
8. <http://ddanchev.blogspot.com/2006/03/5-things-microsoft-can-do-to-secure.html>
9. <http://ddanchev.blogspot.com/2006/02/current-state-of-ip-spoofing.html>
10. <http://www.isotf.org/news/DNS-Amplification-Attacks.pdf>
11. <http://mixter.void.ru/protecting.html>
12. <http://mixter.void.ru/about.html>
13. <http://ddanchev.blogspot.com/2006/02/how-to-win-10000-bucks-until-end-of.html>
14. <http://packetstormsecurity.org/>
15. <http://www.computerworld.com/securitytopics/security/hacking/story/0,10801,109631,00.html>
16. <http://it.slashdot.org/article.pl?sid=06/03/16/1658209>
17. [http://www.cbronline.com/article\\_news.asp?guid=44F6BD06-8855-44AF-98A1-F319FF5895B9](http://www.cbronline.com/article_news.asp?guid=44F6BD06-8855-44AF-98A1-F319FF5895B9)
18. <http://ddanchev.blogspot.com/2006/03/wheres-my-0day-please.html>
19. <http://ddanchev.blogspot.com/2006/02/war-against-botnets-and-ddos-attacks.html>

20. <http://ddanchev.blogspot.com/2006/02/recent-malware-developments.html>
21. <http://news.findlaw.com/hdocs/docs/cyberlaw/usanchetaind.pdf>
22. <http://ddanchev.blogspot.com/2006/02/master-of-infected-puppets.html>
23. <http://www.linuxsecurity.com/docs/malware-trends.pdf>
24. <http://www.patrickmcdaniel.org/pubs/td-5ugj33.pdf>
25. <http://www.ietf.org/html.charters/rpsec-charter.html>
26. <http://ddanchev.blogspot.com/2006/03/are-cyber-criminals-or-bureaucrats.html>
27. <http://ddanchev.blogspot.com/2006/01/how-to-secure-internet.html>
28. <http://ddanchev.blogspot.com/2006/03/5-things-microsoft-can-do-to-secure.html>
29. [http://www.fas.org/irp/congress/2005\\_hr/hhrg109-58.html](http://www.fas.org/irp/congress/2005_hr/hhrg109-58.html)
30. <http://www.intel.com/pressroom/kits/bios/grove/paranoid.htm>
- 262
31. [http://www.theregister.co.uk/2005/02/24/ibm\\_lenovo\\_spooks/](http://www.theregister.co.uk/2005/02/24/ibm_lenovo_spooks/)

32. <http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/interviews/clarke.html>
33. <http://ddanchev.blogspot.com/2006/02/hacktivism-tensions.html>
34. <http://www.washingtonpost.com/wp-dyn/content/article/2006/03/25/AR2006032500020.html>
35. <http://www.linuxsecurity.com/content/view/122340/65/>
36. <http://technorati.com/tag/Security>
37. <http://technorati.com/tag/Information+Security>
38. <http://technorati.com/tag/Internet>
39. <http://technorati.com/tag/Internet2>
40. <http://technorati.com/tag/DDoS>
41. <http://technorati.com/tag/Networking>
42. <http://technorati.com/tag/IPv6>
43. <http://technorati.com/tag/VeriSign>

263

### **Distributed cracking of a utopian mystery code (2006-04-13 15:09)**

If you have missed the opportunity to [1]buy yourself a portable Enigma encryption machine, or didn't know you could devote some of your CPU power while trying to [2]crack unbroken Nazi Enigma ciphers, now is the time to

consider another [3]distributed computing cracking initiative I just came across to - "[4]Assault on the Thirteenth Labour", part of the utopian [5]Perplex City alternate reality game.

More on the [6]story [7]itself :

*" The story centers on a fictional metropolis known as Perplex City. The Receda Cube, a priceless scientific and spiritual artefact, has been stolen and buried somewhere on Earth, and the game offers a real-life \$200,000 reward to whoever can find it. "*

As a matter of fact, ever heard [8]of [9]Hive7? This is where the future is going, as I think [10]virtual worlds

intrigues result in a more quality real life, don't they? Still, it can also result in security problems with [11]stolen virtual goods. The trend, given the popularity of these, will continue to emerge - people, both rich and poor are

putting hard cash into [12]virtual properties and [13]DoS attacks and [14]phishing practices are already gaining popularity as well.

Technorati tags:

[15]Security, [16]Cryptography, [17]Perplex City, [18]Virtual Worlds, [19]Distributed, [20]New Media

1. <http://ddanchev.blogspot.com/2006/04/wanna-get-yourself-portable-enigma.html>

2. <http://ddanchev.blogspot.com/2006/02/get-chance-to-crack-unbroken-nazi.html>

3. [http://en.wikipedia.org/wiki/List\\_of\\_distributed\\_computing\\_projects](http://en.wikipedia.org/wiki/List_of_distributed_computing_projects)
4. [http://homepage.ntlworld.com/t.kirman/PXC/thirteenth\\_labour.htm](http://homepage.ntlworld.com/t.kirman/PXC/thirteenth_labour.htm)
5. <http://www.perplexcity.com/>
6. <http://story.perplexcity.com/>
7. [http://en.wikipedia.org/wiki/Perplex\\_City](http://en.wikipedia.org/wiki/Perplex_City)
8. <http://ddanchev.blogspot.com/2006/03/visualization-in-security-and-new.html>
9. <http://www.hive7.com/>
10. <http://www.virtualworldsreview.com/>
11. <http://ddanchev.blogspot.com/2006/04/insider-fined-870.html>
12. <http://news.bbc.co.uk/1/hi/technology/3138456.stm>
13. [http://news.netcraft.com/archives/2005/11/14/malware\\_knocks\\_virtual\\_world\\_offline.html](http://news.netcraft.com/archives/2005/11/14/malware_knocks_virtual_world_offline.html)
14. [http://terranova.blogs.com/terra\\_nova/2005/09/virtual\\_world\\_p.html](http://terranova.blogs.com/terra_nova/2005/09/virtual_world_p.html)
15. <http://technorati.com/tag/Security>
16. <http://technorati.com/tag/Cryptography>

17. <http://technorati.com/tag/Perplex+City>
18. <http://technorati.com/tag/Virtual+Worlds>
19. <http://technorati.com/tag/Distributed>
20. <http://technorati.com/tag/New+Media>

264

### **Fighting Internet's email junk through licensing (2006-04-14 19:18)**

Just came across this [1]story at [2]Slashdot, interesting approach :

*" China has introduced [3] regulationsthat make it illegal to run an email server without a licence.*

*The new*

*rules, which came into force two weeks ago, mean that most companies running their own email servers in China*

*are now breaking the law. The new email licensing clause is just a small part of a new anti-spam law formulated by*

*China's Ministry of Information Industry (MII). "*

While the commitment is a remarkable event given [4]China's booming [5]Internet population – among the

main reasons Google had to somehow [6]enter [7]China's search market and take market share from Baidu.com

– you don't need a mail server to [8]disseminate spam and phishing attacks like it used to be in the old days. You



[9]need [10]botnets, namely, going through [11]CME's List, you would see how the majority of [12]today's malware

is loaded with build-in SMTP engine, even offline/in-transit/web email harvesting modules.

You can often find China on the top of every recently released spam/[13]phishing/botnet trends summary,

which doesn't mean Chinese Internet users are insecure – just unaware. What you can do is educate the masses to

secure the entire population, and stimulate the growth of the local security market that everyone is so desperately

trying to tap into.

Moreover, I doubt you can regulate the type of Internet users still trying to [14]freely access information, again with

the wrong attitude in respect to security :

*".. prohibiting use of email to discuss certain vaguely defined subjects related to 'network security' and 'information security', and also reiterate that emails which contain content contrary to existing laws must not be copied or forwarded. Wide-ranging laws of this nature have been used against political and religious dissenters in the past. "*

It's like legally justifying the country's [15]censorship practices through introducing the law, whereas I feel

"network security" and "information security" [16]attacks outside the homeland get favored, compared to [17]internal ones, don't you?

Forbidden fruits turn into dangerous desires on the majority of occasions, and you just can't control that,

what's left to censor it.

Technorati tags:

265

[18]Security, [19]Malware, [20]Spam, [21]Phishing,  
[22]China

1. <http://www.vnunet.com/vnunet/news/2154063/china-outlaws-outlook>
2. <http://yro.slashdot.org/yro/06/04/14/1459238.shtml>
3. <http://www.isc.org.cn/20020417/ca346007.htm>
4. <http://www.internetworldstats.com/asia.htm#cn>
5. <http://www.internetworldstats.com/articles/art045.htm>
6. <http://ddanchev.blogspot.com/2006/02/chinese-internet-censorship-efforts.html>
7. <http://blog.searchenginewatch.com/blog/060403-105558>
8. <http://www.email-policy.com/Spam-black-lists.htm>
9. <http://ddanchev.blogspot.com/2006/02/master-of-infected-puppets.html>
10. <http://ddanchev.blogspot.com/2006/02/war-against-botnets-and-ddos-attacks.html>
11. <http://cme.mitre.org/data/list.html>

12. <http://packetstormsecurity.org/papers/general/malware-trends.pdf>
13. <http://ddanchev.blogspot.com/2006/03/anti-phishing-toolbars-can-you-trust.html>
14. <http://ddanchev.blogspot.com/2006/02/chinese-internet-censorship-efforts.html>
15. <http://edition.cnn.com/interactive/world/0603/explainer.china.internet/frameset.exclude.html>
16. <http://ddanchev.blogspot.com/2006/02/hacktivism-tensions.html>
17. <http://seclists.org/lists/isn/1999/Dec/0010.html>
18. <http://technorati.com/tag/Security>
19. <http://technorati.com/tag/Malware>
20. <http://technorati.com/tag/Spam>
21. <http://technorati.com/tag/Phishing>
22. <http://technorati.com/tag/China>

266

### **Would somebody please buy this Titan 1 ICBM Missile Base? (2006-04-18 13:44)**

I feel that no matter how much you [1]try to bypass the [2]intermediary, it would continue to remain the place for

anything auction - [3]0day vulnerabilities, [4]Enigma encryption machines, and now a [5]Titan 1 ICBM Missile

Base,

is for sale at Ebay for the N time. Bari Hotchkiss listed the characteristics of the underground fortress as :

- *Hardened buildings built to withstand One megaton nuclear blast within three thousand feet*
- *Wall thicknesses up to fourteen feet*
- *Thousands of feet of connecting tunnels*
- *Paved roads. Security fencing*

Trying to auction it [6]again, as he seems to own the [7]facility, it beats [8]The Bunker in respect to a wide

range of physical/electronic attack based security possibilities, and has the potential to turn into the perfect data

center with enough space for war rooms on every level.

As [9]Gene Spafford once put it :

*" The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards - and even then I have my doubts."*

and you would probably need a network connection of some kind to make use if it – that means insecurities

posed out of open and hard to control external networks.

I've once mentioned how [10]nuclear weapons aren't the type of central military thinking problem the way

they used to be during the Cold War's arms race, as there are many more emerging threats to consider, such as EMP, and [11]Space warfare, but that's hell of an offer for a post-ColdWar underground complex, isn't it?

Some resources worth taking a look at :

[12]19 Ways to Build Physical Security into a Data Center

[13]Data Center : Securing Server Farms - Solution Reference Network Design

[14]Data Center Security Associate Certificate Recommended Reading

Technorati tags:

267

[15]Security, [16]ICBM, [17]Data Center, [18]Missile Base

1. <http://base.google.com/>
2. <http://www.ebay.com/>
3. <http://ddanchev.blogspot.com/2005/12/0bay-how-realistic-is-market-for.html>
4. <http://ddanchev.blogspot.com/2006/04/wanna-get-yourself-portable-enigma.html>
5. [http://cgi.ebay.com/Titan-1-ICBM-Missile-Base-Located-in-Washington-State\\_W0QQitemZ4455060285QQcategoryZ1607QQrdZ1QQ](http://cgi.ebay.com/Titan-1-ICBM-Missile-Base-Located-in-Washington-State_W0QQitemZ4455060285QQcategoryZ1607QQrdZ1QQ)

6. <http://slashdot.org/articles/04/03/14/0545202.shtml?tid=103&tid=98&tid=99>
7. <http://www.wired.com/news/culture/0,1284,47577,00.html>
8. <http://www.thebunker.net/our-facilities/data.htm>
9. <http://homes.cerias.purdue.edu/~spaf/>
10. <http://ddanchev.blogspot.com/2006/02/who-needs-nuclear-weapons-anymore.html>
11. <http://ddanchev.blogspot.com/2006/03/is-space-warfare-arms-race-really.html>
12. <http://www.csoonline.com/read/110105/datacenter.html>
13. [http://www.cisco.com/application/pdf/en/us/guest/netso/ns304/c649/ccmigration\\_09186a008014edf3.pdf](http://www.cisco.com/application/pdf/en/us/guest/netso/ns304/c649/ccmigration_09186a008014edf3.pdf)
14. <http://www.idcp.org/security.htm>
15. <http://technorati.com/tag/Security>
16. <http://technorati.com/tag/ICBM>
17. <http://technorati.com/tag/Data+Center>
18. <http://technorati.com/tag/Missile+Base>

268

**Spotting valuable investments in the information security market (2006-04-18 19:15)**

Back in [1]January I mentioned the possible acquisition of SiteAdvisor in my "[2]Look who's gonna cash for evaluating the maliciousness of the Web?" post and it seems [3]McAfee have realized the potential of this social-networking

powered concept on a wide scale, and recently [4]acquired [5]SiteAdvisor – this was meant to happen one way or

another and with risk of being over-enthusiastic I feel I successfully spotted this one.

Next to SiteAdvisor's pros and cons that I commented on, I also provided a resourceful overview of some of

the current malware crawling projects out there, to recently find out that WebRoot finally went public with the

[6]Phileas spyware crawler, and that Microsoft's [7]Strider Crawler came up with the [8]Typo-Control project – great

idea as a matter of fact. What are some of the current/future trends in the information security industry? Are the

recent flood of acquisitions the result of cheaper hardware and the utilization of open-source software, thus cutting

costs to the minimum while the idea still makes it to the market?

Have both, entry and exit barriers totally vanished so that anyone could get aspired of becoming a vendor

without the brand at the first place? Excluding the big picture, it is amazing how uninformed both, end and corporate

users are, yet another lack of incentive for security vendors to reach another level of solutions – if it ain't broken, don't improve it.

Moreover, what would the effect be of achieving the utopian 100 % security on both, the market and the

world's economy? On one hand we have "the worst year" of [9]cybercrime, whereas [10]spending and [11]salaries

are booming, and they should be as the not knowing how much security is enough, but trying to achieve the most

secured state is a driving factor for decades to come.

The bottom line is, the more insecurities, the more security spending, the higher the spending, the higher the

growth, and with increasing purchasing power, corporate R &D, and government initiatives you have a fully working

economic model – going to war, or seeing terrorists everywhere is today's driving force for military/intelligence

spending compared to the "Reds are everywhere" propaganda from both camps of course, back in the Cold War

period. Fighting with [12]inspired [13]bureaucrats is always an issue as well.

The [14]Ansoff's Product/Market Matrix often acts as the de-facto standard for developing business opportuni-

ties, that is, of course, if you're not lead by a visionary aim, promote an internal "everyday startup" atmosphere to



stimulate creativity, or [15]benchmark against competitors. On the majority of occasions a security vendor is

looking for ways to diversify its solutions' portfolio, thus taking advantage of re-introduced product life cycles and new sources for revenues.

While there should be nothing wrong with that given a vendor is actually providing a reliable solution and

support with it, I often argue on how marketable propositions centric business model is not good for the long-term

competitiveness of the company in question.

269

It's the judgement and competitors [16]myopia that I'm talking about. In respect to the current information security market trends, or let's pick up the anti virus solutions segment, that means loosing sight of the big picture

with the help of the mainstream media – cross referenced malware names, "yet another" malware in the wild, or supposed to be Russian hacker selling his soul for E-gold(cut the stereotypes here and go through the majority of

recent statistics to see where all that phishing, spam and malware is coming from), is a common weakness of a

possible decision-maker looking for acquisitions. Focusing on both, current trends, and current competitions is the

myopia that would prevent you from sensing the emerging ones, the ones that would improve your competitiveness

at any time of execution of course.

The way we have been witnessing an overall shift towards a services based world economy in comparison to

a goods based one, in the information security market services or solutions will inevitably proliferate in the upcoming

future. When was the last time you heard someone saying " *I don't need an anti-virus scanner, but an anti-virus solution, what's yours and how is it differentiated from the others I'm aware of*"? Un-informed decisions, quick and cheap way to get away with the "security problem", or being totally brainwashed by a vendor's salesforce would result in enormous long-term TCO(total cost of ownership) problems, given someone actually figures a way to make

the connection in here.

Some time ago, I came across a great article at CSOOnline.com "[17]2 Vendor Megatrends and What They

Mean to You" giving insight on two trends, namely, consolidation of security providers and convergence – the

interception between IT and physical security. And while it's great in respect to covering these current trends, I feel

the article hasn't mentioned the 3rd one - Diversification. An excerpt :

" *One trend is consolidation. "We're seeing the bigger players buying out many of the smaller companies. And I think the largest of the security firms are looking to provide a full range of enterprise services," says C. Warren Axelrod, director of global information security at Pershing, a Bank of*

*New York Securities Group company. "The larger firms, like Internet Security Systems, Symantec and Computer Associates, are buying in many areas to complement*

*what they have. They're basically vying for control of the security space." Axelrod is dead on, and consolidation is just as rampant among physical security vendors as it is in the IT world. "*

I feel consolidation is happening mainly because different market segments are constantly getting crowded

and mainly because it's very, very hard to get a name in the information security market these days, so instead of

run for your own IPO, compete against market players whose minor modification may ruin your entire idea, you'd

better get acquired one way or another. [18]@stake is an example of how skilled HR runs away from the acquirer, at

least for me counting the HR as the driving force besides the brand.

More from the article :

*" The second trend is convergence—the confluence of IT and physical security systems and vendors—which, in*

*some sense, is another form of consolidation, only it's happening across the line that historically divided those two*  
270

*worlds. "*

Tangible security is often favored by investors as it targets the masses, and the most visible example besides

perimeter based defenses are the hardware appliances themselves. These days, there isn't a single anti virus, anti

spam or anti spyware solution provider without a hardware appliance, but what's to note is how their OEM agree-

ments are still working and fully applicable, it's all about greed, or let's avoid the cliché and say profit maximization -

whatever the market requires the vendors deliver!

Very in-depth article, while I can argue that vendors are so desperate to "consolidate bids" on a national level, as they usually try to get as big part of the pie as possible. What's else to note is that the higher the market

transparency, the more competitive the environment, thus greater competition which is always useful for the final

user. In respect to heterogeneity and homogeneity of security solutions, and all-in-one propositions, the trade-offs are

plain simple, cut total TCO by using a single vendor, get your entire infrastructure breached into by an attacker that

would sooner or later find a vulnerability in it - find the balance and try to avoid the myth that complexity results in insecurities, as it's a unique situation every time.

What we're witnessing [19]acquisition-to-[20]solution turn-around periods of several months in response to

an emerging market - the IM one, [21]mobile anti-virus scanners [22]seem [23]to be the "next big thing", whereas it would take quite some time for this segment to develop, still you'd better be among the first to respond to the

interest and the fact that there are more mobile phones capable of getting infected with a virus, than PCs out there

- 3G, 4G, mobile banking would fuel the growth even more, and these are just among the few issues to keep in mind.

In a previous [24]post, I also mentioned on a creative use of security intelligence information in Sophos's [25]Zombie

Alert service, and a product-line extensions, namely McAfee's bot killing system. What no one pictured would

happen is emerging these days - vulnerabilities turning into IP and the overall commercialization of the [26]security

vulnerabilities market, and [27]getting paid for getting hacked is a growing trend as well - much more's to come for sure.

### **The secrets to successful acquisitions?**

- retain the HR that came with it, and better put something on the table at the first place

- don't try to cannibalize the culture there, Flickr is the perfect example out of the security market

- go beyond the mainstream media sources, and PR releases, use open source competitive intelligence tools in order

not to miss an opportunity

- attend as much cons as possible to keep track of who's who and where's the industry heading to

- cost-effectively keep in touch with researchers, and an eye on their blogs, you never know who would be your early

warning system for business development ideas

Try to stay on the top of security, not in line with it.

271

Technorati tags:

[28]Security, [29]Information Security, [30]SiteAdvisor,  
[31]McAfee, [32]Investing, [33]Investment, [34]Market

Trends, [35]Economics

1. <http://ddanchev.blogspot.com/2006/01/januarys-security-streams.html>
2. <http://ddanchev.blogspot.com/2006/02/look-whos-gonna-cash-for-evaluating.html>
3. [http://www.mcafee.com/us/about/press/consumer/2006/20060403\\_050000\\_q.html](http://www.mcafee.com/us/about/press/consumer/2006/20060403_050000_q.html)
4. [http://blog.siteadvisor.com/2006/04/taking\\_siteadvisor\\_to\\_the\\_next.shtml](http://blog.siteadvisor.com/2006/04/taking_siteadvisor_to_the_next.shtml)
5. <http://www.siteadvisor.com/>
6. <http://www.webroot.com/resources/phileas>
7. <http://research.microsoft.com/sm/strider/>
8. <http://research.microsoft.com/Typo-Patrol/>
9. <http://ddanchev.blogspot.com/2006/01/why-we-cannot-measure-real-cost-of.html>

10. <http://ddanchev.blogspot.com/2006/01/fbis-2005-computer-crime-survey-whats.html>
11. <http://www.sans.org/salary2005/>
12. <http://ddanchev.blogspot.com/2006/03/are-cyber-criminals-or-bureaucrats.html>
13. <http://news.bbc.co.uk/2/hi/americas/4655196.stm>
14. [http://www.marketingteacher.com/Lessons/lesson\\_ansoff.htm](http://www.marketingteacher.com/Lessons/lesson_ansoff.htm)
15. [http://en.wikipedia.org/wiki/Competitor\\_analysis](http://en.wikipedia.org/wiki/Competitor_analysis)
16. [http://en.wikipedia.org/wiki/Marketing\\_myopia](http://en.wikipedia.org/wiki/Marketing_myopia)
17. [http://www.csoononline.com/read/030106/vendor\\_megatrends.html](http://www.csoononline.com/read/030106/vendor_megatrends.html)
18. <http://www.atstake.com/>
19. <http://ddanchev.blogspot.com/2006/01/whats-potential-of-im-security-market.html>
20. <http://www.networkworld.com/news/2006/041006-symantec-im-security.html>
21. <http://mobile.f-secure.com/>
22. <http://www.scmagazine.com/uk/news/article/554109/kaspersky+introduces+mobile+anti-virus+software>
23. [http://www.symantec.com/Products/enterprise?c=prodinfo&refId=921&ln=en\\_AU](http://www.symantec.com/Products/enterprise?c=prodinfo&refId=921&ln=en_AU)

24. <http://ddanchev.blogspot.com/2006/02/war-against-botnets-and-ddos-attacks.html>
25. [http://photos1.blogger.com/blogger/1933/1779/1600/sophos\\_zombie\\_alert\\_service.9.png](http://photos1.blogger.com/blogger/1933/1779/1600/sophos_zombie_alert_service.9.png)
26. <http://ddanchev.blogspot.com/2006/03/wheres-my-0day-please.html>
27. [http://ddanchev.blogspot.com/2006/03/getting-paid-for-getting-hacked\\_17.html](http://ddanchev.blogspot.com/2006/03/getting-paid-for-getting-hacked_17.html)
28. <http://technorati.com/tag/Security>
29. <http://technorati.com/tag/Information+Security>
30. <http://technorati.com/tag/SiteAdvisor>
31. <http://technorati.com/tag/McAfee>
32. <http://technorati.com/tag/Investing>
33. <http://technorati.com/tag/Investment>
34. <http://technorati.com/tag/Market+Trends>
35. <http://technorati.com/tag/Economics>

272

### **Digital forensics - efficient data acquisition devices (2006-04-20 17:23)**

[1]Digital forensics have always been a hot market segment, whereas the need for a reliable network based forensics



model given main [2]Internet's insecurities such as [3]source address spoofing and the lack of commonly accepted

security events reporting practices is constantly growing as well. Information acquisition, analysis and interpretation

in the most reliable and efficient way is often among the desired outcome – and of course figure out what has been

happening at a given historical moment in time or in real-time if applicable.

In a previous post related to "[4]Detecting intruders and where to look for" I mentioned lots of resources re-

garding the topic, and tools to take advantage of, if in need. In respect to cell phones and various related [5]privacy

issues, excluding the physical forensic analysis that could be successfully performed, there's a growing discussing on

whether a "suspect's" physical location should be revealed though a mobile-phone carrier – segmented requests are the most efficient and socially-conscious ones I think.

Today I came across to "[6]Logicube CellIDEK" a portable handset data extraction kit :

*" The portable CellIDEK® acquires data from over 160 of the most popular cell phones and PDA's. Built to per-*

*form in the field (not just in the lab), investigators can immediately gain acces to vital information. This saves days of waiting for crucial data to come back from a crime lab. The CellIDEK software automatically performs forensic*

*extraction of the following data: Handset Time and Date, Serial Numbers (IMEI, IMSI), Dialed Calls, Received Calls, Phonebook (both handset and SIM), SMS (both handset and SIM), Deleted SMS from SIM, Calendar, Memos, To Do Lists, Pictures, Video, and Audio."*

Nothing surprising as there are many other freeware applications/ways to do [7]cell phone forensics ([8]full

list can be found at Sergio Hernando's blog), but what made me an impression was its usefulness by covering over

160 models, portability due to its size and capabilities, and that up to 40 adapters may be stored in the system's

built-in rack. Some challenges I see to today's forensic investigators are the sophistication of publicly available

encryption/steganographic tools, the Internet acting as a online HDD opening opportunities for dead-drop places,

and communications that went over [9]covert channels.

On my wislist however, has always been the company's [10]Forensic MD5, as it basically "swallows" data in a

timely manner – a bad toy in the hands of a [11]insider going beyond average types of removable media, and in mo-

ments where minutes count. As a matter of fact, a forensic investigator's sophistication and expertise doesn't really

count when the [12]Mafia is still catching up on how to encrypt. Still, I'm convinced how some of his "operatives"

are into far more sophisticated methods of communication than he is.

Check out some more resources, and case studies on the topic as well :

273

[13]How to Become a Cyber-Investigator

[14]SANS Reading Room - Forensics

[15]Digital Forensics Tool Testing Images

[16]Computer Forensics for Lawyers

[17]Forensic Analysis of the Windows Registry

[18]Forensic Computing from a Computer Security perspective

[19]Guidelines on PDA Forensics

[20]Forensic Examination of a RIM (BlackBerry) Wireless Device

[21]WebMail Forensics

[22]iPod Forensics

[23]Digital Music Device Forensics

[24]Forensics and the GSM mobile telephone system

[25]List of Printers Which Do or Don't Print Tracking Dots

[26]Metasploit Anti-forensics homepage

## **UPDATE** - Sites that picked up the story

[27]LinuxSecurity.com

Technorati tags:

[28]Security, [29]Forensics, [30]cyber-crime, [31]Mobile Phone

1. [http://en.wikipedia.org/wiki/Computer\\_forensics](http://en.wikipedia.org/wiki/Computer_forensics)
2. [http://ddanchev.blogspot.com/2006/04/on-insecurities-of-internet\\_13.html](http://ddanchev.blogspot.com/2006/04/on-insecurities-of-internet_13.html)
3. <http://ddanchev.blogspot.com/2006/02/current-state-of-ip-spoofing.html>
4. <http://ddanchev.blogspot.com/2006/02/detecting-intruders-and-where-to-look.html>
5. <http://ddanchev.blogspot.com/2006/03/privacy-issues-related-to-mobile-and.html>
6. [http://www.logicubeforensics.com/products/hd\\_duplication/celldek.asp](http://www.logicubeforensics.com/products/hd_duplication/celldek.asp)
7. <http://csrc.nist.gov/publications/nistir/nistir-7250.pdf>
8. <http://www.sahw.com/wp/archivos/2006/04/09/analisis-forense-de-telefonos-moviles-y-tarjetas-sim>
9. <http://gray-world.net/>
10. [http://www.logicubeforensics.com/products/hd\\_duplication/md5.asp](http://www.logicubeforensics.com/products/hd_duplication/md5.asp)

11. <http://ddanchev.blogspot.com/2005/12/insiders-insights-trends-and-possible.html>
12. [http://dsc.discovery.com/news/briefs/20060417/mafiaboss\\_tec.html](http://dsc.discovery.com/news/briefs/20060417/mafiaboss_tec.html)
13. <http://certification.about.com/cs/securitycerts/a/compforensics.htm>
14. <http://www.sans.org/rr/whitepapers/forensics/>
15. <http://dfft.sourceforge.net/>
16. [http://www.craigball.com/cf\\_vcr.pdf](http://www.craigball.com/cf_vcr.pdf)
17. <http://www.forensicfocus.com/forensic-analysis-windows-registry>
18. <http://www.diva-portal.org/liu/abstract.xsql?dbid=2421>
19. <http://csrc.nist.gov/publications/nistpubs/800-72/sp800-72.pdf>
20. <http://www.rh-law.com/ediscovery/Blackberry.pdf>
21. <http://www.blackhat.com/presentations/bh-usa-03/bh-us-03-akin.pdf>
22. [https://www.cerias.purdue.edu/tools\\_and\\_resources/bibtex\\_archive/archive/2005-13.pdf](https://www.cerias.purdue.edu/tools_and_resources/bibtex_archive/archive/2005-13.pdf)
23. [https://www.cerias.purdue.edu/tools\\_and\\_resources/bibtex\\_archive/archive/2005-27.pdf](https://www.cerias.purdue.edu/tools_and_resources/bibtex_archive/archive/2005-27.pdf)

24.

<http://www.utica.edu/academic/institutes/ecii/publications/articles/A0658858-BFF6-C537-7CF86A78D6DE746D.p>

274

df

25. <http://www.eff.org/Privacy/printers/list.php>

26. <http://metasploit.com/projects/antiforensics/>

27. <http://www.linuxsecurity.com/content/view/122524/65/>

28. <http://technorati.com/tag/Security>

29. <http://technorati.com/tag/Forensics>

30. <http://technorati.com/tag/cyber-crime>

31. <http://technorati.com/tag/Mobile+Phone>

275

### **The anti virus industry's panacea - a virus recovery button (2006-04-20 20:07)**

[1]Just when I thought I've seen everything when it comes to  
[2]malware, I was wrong as a PC vendor is trying

to desperately position itself as one offering a feeling of  
security with the idea to strip its product and lower the

customer price. The other day I came across to a fancy ad  
featuring Lenovo's ThinkVantage [3]Virus Recovery Button,

and promoting its usefulness even when there's no AV  
solution in place :

*" Rescue and Recovery is a one button recovery and restore solution that includes a set of self recovery tools to help users diagnose, get help and recover from a virus or other system crashes quickly, even if the primary operating system will not boot and you are remote from your support team. "*

The [4]video ad is indeed fascinating, and while their [5]Embedded Security Subsystem 2.0 " *locks your sensi-*

*tive data behind hardware-based encryption"*, you'd better take advantage of their [6]utilities options and try to avoid such a weak positioning in respect to malware. The Virus Recovery Button seems to be directly targeting the

masses and totally removing the complexity issue by introducing a button-based solution to malware – dangerous as

backups and their idea could have proven useful during the first [7]generations of malware.

[8]Anti virus signatures, response time, and various other [9]proactive malware prevention approaches such

as, IPS, buffer overflow protection are among today's most widely discussed approaches when dealing with malware,

and of course, [10]the principle of least privilege to user accounts. But why the anti virus button when it can be

an anti-hacker one? I feel they'd better stick to their OEM agreements and find other ways to achieve competitive

advantage in pricing than providing a false sense of security.

In my recent "[11]Malware - future trends" research I mentioned on the fully realistic scenario of having your security solution turn into a security problem itself. While this is nothing new, in this case we have a misjudged

security proposition, as recovering to a pre-infection state doesn't necessarily mean confidentiality of sensitive

personal/financial information wouldn't be breached by the time the user is aware of the infection, if it ever happens

of course.

Moreover, Lenovo was recently under [12]scrutiny as "*The U.S.-China Economic Security Review Commission*

276

*(USCC) argues that a foreign intelligence like that of the Communist Party of China (CPC) can use its power to get Lenovo to equip its machines with espionage devices. Lenovo has strongly declined that it is involved in any such*

*activities"*, and while they eventually reached a consensus on using the machines on unclassified systems only, it doesn't mean they aren't exposed to a wide variety of threats going beyond China backdooring them, such as

[13]Zotob over border-screening systems at airports.

As a matter of fact, the rival PC/notebook propositions might still be owned by U.S companies, but are mostly

assembled in China these days - too much hype for nothing.

**UPDATE** - Sites that picked up the post

[14]LinuxSecurity.com



[15]MalwareHelp.org

Technorati tags:

[16]Security, [17]Malware, [18]Anti-virus, [19]Lenovo,  
[20]Data Recovery

1.  
<http://photos1.blogger.com/blogger/1933/1779/1600/computer%20virus.jpg>
2. <http://ddanchev.blogspot.com/2006/01/malware-future-trends.html>
3.  
<http://www.pc.ibm.com/us/think/thinkvantagetech/rescuerecovery.html>
4.  
[http://www.pc.ibm.com/us/media/notebooks/thinkpad/virus\\_wmv.html](http://www.pc.ibm.com/us/media/notebooks/thinkpad/virus_wmv.html)
5.  
[http://www.thinkwiki.org/wiki/Embedded\\_Security\\_Subsystem](http://www.thinkwiki.org/wiki/Embedded_Security_Subsystem)
6. [https://www-1.ibm.com/products/hardware/configurator/na/ui/launchTopLevelConfig.wss?W7P3850=1&base=252901U&cntry=840&lang=en\\_US&amp;amp;launch\\_type=LMBI&rattyp](https://www-1.ibm.com/products/hardware/configurator/na/ui/launchTopLevelConfig.wss?W7P3850=1&base=252901U&cntry=840&lang=en_US&amp;amp;launch_type=LMBI&rattyp)
7. <http://www.cioupdate.com/article.php/3598621>
8. <http://ddanchev.blogspot.com/2006/01/why-relying-on-virus-signatures-simply.html>

9. [http://www.viruslist.com/en/downloads/vlpdfs/wp\\_nikishin\\_preactive\\_en.pdf](http://www.viruslist.com/en/downloads/vlpdfs/wp_nikishin_preactive_en.pdf)
10. <http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/luawinxp.msp>
11. <http://packetstormsecurity.org/papers/general/malware-trends.pdf>
12. <http://www.dailytech.com/article.aspx?newsid=1497>
13. <http://www.wired.com/news/technology/0,70642-0.html>
14. <http://www.linuxsecurity.com/content/view/122525/65/>
15. <http://www.malwarehelp.org/news/article-3390.html>
16. <http://technorati.com/tag/Security>
17. <http://technorati.com/tag/Malware>
18. <http://technorati.com/tag/Anti-virus>
19. <http://technorati.com/tag/Lenovo>
20. <http://technorati.com/tag/Data+Recovery>

277

### **Why's that radar screen not blinking over there? (2006-04-24 15:39)**

Two days ago, the Russian News & Information Agency - Novosti, reported on how "[1]Russian bombers flew

undetected across Arctic" more from the article :

*" Russian military planes flew undetected through the U.S. zone of the Arctic Ocean to Canada during recent*

*military exercises, a senior Air Force commander said Saturday. The commander of the country's long-range strategic*

*bombers, Lieutenant General Igor Khvorov, said the U.S. Air Force is now investigating why its military was unable to detect the Russian bombers. They were unable to detect the planes either with radars or visually," he said. "*

[2]SpaceWar.com, and [3]several other sites/[4]agencies also picked up the story, still its truthfulness, exclud-

ing the lack of coverage, can always be questioned, as " *by the end of the year, two more [5]Tu-160s will be*

*commissioned for the long-range strategic bomber fleet, Khorov said. "* So, while I agree with him on the visual confirmation issue, such an achievement is hell of an incentive for commissioning more planes, isn't it? Moreover,

should the what used to be, the world's largest radar - [6]The Over-The-Horizon Backscatter Radar have been

[7]scrapped given Iran's (and not only) [8]nuclear ambitions, or the ongoing [9]space warfare doctrine would be the

logical successor in here?

Let's for instance assume it actually happened, and take the reverse approach - it actually happened in Russia

too, back in 1987, and it wasn't a senior air force commander that did it, if he did, but 19 years old

[10]Mathias Rust

who landed on the Red Square itself.

More details will follow for sure, so stay tuned, meanwhile take a look at Google Earth's Community [11]spot

link on Mathias's landing.

## **UPDATE**

[12]Nice article on the topic, and a great quote as well "*Scanning containers full of sneakers for a 'nuke in a box' is not a really thoughtful thing.*"

Technorati tags:

[13]Military, [14]Radar, [15]Bomber

1. <http://en.rian.ru/russia/20060422/46792049.html>
2. [http://www.spacewar.com/reports/Russian\\_Bombers\\_Flew\\_Un\\_detected\\_Across\\_Arctic.html](http://www.spacewar.com/reports/Russian_Bombers_Flew_Un_detected_Across_Arctic.html)
3. <http://www.flightglobal.com/Articles/2006/04/24/Navigation/177/206145/Russians+claim+bomber+flights+over+US+territory+went.html>
4. [http://www.interfax.ru/e/B/politics/28.html?id\\_issue=11502888](http://www.interfax.ru/e/B/politics/28.html?id_issue=11502888)
5. <http://en.wikipedia.org/wiki/Tu-160>

6. <http://www.fas.org/nuke/guide/usa/airdef/an-fps-118.htm>
7. [http://www.boston.com/news/local/maine/articles/2005/02/21/maines\\_cold\\_war\\_era\\_radar\\_system\\_being\\_scrapped/](http://www.boston.com/news/local/maine/articles/2005/02/21/maines_cold_war_era_radar_system_being_scrapped/)
8. <http://ddanchev.blogspot.com/2006/02/who-needs-nuclear-weapons-anymore.html>
9. <http://ddanchev.blogspot.com/2006/03/is-space-warfare-arms-race-really.html>
10. [http://en.wikipedia.org/wiki/Mathias\\_Rust](http://en.wikipedia.org/wiki/Mathias_Rust)
11. <http://bbs.keyhole.com/ubb/showthreaded.php?Number=197100>
12. <http://www.washingtonpost.com/wp-dyn/content/article/2006/04/14/AR2006041401369.html>
13. <http://technorati.com/tag/Military>
14. <http://technorati.com/tag/Radar>
15. <http://technorati.com/tag/Bomber>

279

## **25 ways to distinguish yourself - and be happy? (2006-04-24 17:45)**

Totally out of the security world, yet very relevant inspirational tips for all readers feeling down, or looking for more sources of self-esteem. I've always believed that among the most important key factors for leadership is the ability to

know yourself, and to understand the time dimensions of failure – it's just a temporary event whenever it happens

to occur. I also often debate on the pros and cons of corporate citizenship with friends, and try to emphasize on the

mobility of today's workforce – at least the way I see it. Is there any use of such an approach these days, and how

should an enterprise go when attracting and retaining its most valuable HR assets? Does the individual really count at the bottom line?

I think assets with attitude are the most valuable ones, given they never stop self-developing themselves. Go-

ing back to this very positive "[1]manifesto" "*You don't have to motivate me, just stop demotivating me*" type of attitude is what you can greatly enjoy in these tips. Extremely well written key points, especially that "*being part of the commodity crowd erodes your value*", so true. These get [2]updated all the time, so add them to your own unique ways of distinguishing yourself – and being happy? :)

01. Care as if it's your own
02. Do your daily work with passion
03. Build strong relationships
04. Dream big!
05. Set the right expectations
06. Ask for help

07. Celebrate small victories
08. Set higher standards
09. Know your values
10. Pursue right memberships
11. Help people help themselves
12. Be a reader
13. Plan by outcomes
14. Think long-term
15. Embrace uncertainty with ease
16. Ask the right questions
17. Engage with a coach
18. Re relevant
19. Get back on your feet fast!
20. Lead a volunteer effort
21. Balance innovation and continuous improvement
22. Learn to sell – your skills, not your soul or at least not on parts
23. Learn systems thinking
24. Walk away from free
25. Influence the influencers

1.

[http://www.changethis.com/17.25WaystoDistinguish/download/?screen=0&action=download\\_manifesto](http://www.changethis.com/17.25WaystoDistinguish/download/?screen=0&action=download_manifesto)

2. <http://blog.lifebeyondcode.com/blog/Distinguishyourself>

280

## **Wild Wild Underground (2006-04-25 13:05)**

Where's the real underground these days, behind the shadows of the [1]ShadowCrew, the revenge of the now,

for-profit script kiddies, or in the slowly shaping real Mafia's online ambitions? Moreover, is all this activity going on behind the Dark Web, or the WWW itself? Go through this fresh overview, emphasizing on today's script kiddies,

0days as a commodity, malware and DDoS on demand on the WWW itself, and perhaps a little bit of vendors'

tolerated FUD.

In a previous post, I mentioned on the existence of the [2]International Exploits Shop, the **Xshop**, basically a

web module where 0days, and service support in terms of videos, PHP-based configuration etc. are provided to

anyone willing to get hold of a 0day/zero-day vulnerability – scary stuff, yet truly realistic concept that's directly

bypassing today's infomediaries that purchase vulnerabilities.

I must admit I didn't do homework well enough to figure out that the Hack Shop has been changing quite



some places for the last two years and having offered many other vulnerabilities, going beyond what I came across

to two months ago – the Internet offers a much wider set of potential buyers than from the three intermediaries

for the time being. As a reader gave me a hint, in the future images would protect that type of pages from crawling

activities, and it's interesting to note that previous versions of the shop were doing exactly the same, while the last

one I got tipped about, was using text on its pages. What's also important to mention is that these are the public

propositions, ones placed on the WWW, and not the Dark Web, the one behind closed doors. Last month, [3]Sophos

[4]mentioned on the existence of a multi-exploit kit for an unbelievably cheap price :

*" A Russian website is selling a spyware kit for \$15. The website promises an easy-to-deploy spyware that only*

*requires users to trick their victims into visiting a malicious website. The website even offers technical support. Carole Theriault, senior security consultant at Sophos, says such websites invite script kiddies and other unskilled would-be hackers into the world of cybercrime for profit. "*

281

Rather interesting, [5]WebSense Security Labs looked further, came up with the screenshots from the site itself, cut the last screenshot you can clearly see here ( *Disable adobe acrobat web capture, Disable opera user, Kill frame, Location lock, Referrer lock*) but again spread the rumour of

multi-exploit kit for sale at **\$15**, of course for entering the for-profit cyber crime business – a little bit of FUD, sure, but the sellers aren't still that very desperate I think.

So, I decided to look even further and now can easily conclude – it depends where you're buying it from, I

mean even the official site sells it at a price that way too high for an average script kiddie to get hold of multi-exploits pack – whether outdated or not can be questioned as well.

So, **the kit officially goes for \$300** and, **\$25 for updates**, I also came across it **for \$95**, but I bet they are a lot of people looking for naive wannabe exploiters out there. As you can see on these screenshots, it has the ability to encrypt HTML pages, parts of the page, and take precautions

for curious folks trying to figure out more about the page in question, and it makes me wonder on how well would

malicious HTML detection would perform here, if it does?

What's the outcome – script kiddies with attitude are basically compiling toolsets of old exploits and building

all-in-one malware kits. As you can even see, they are lazy enough not to keep an eye on its detection status, a sign

of "growing" business for sure, yet the "underground" seems to [6]Ph34r going to the Opera , so take your note.

I recently came across to a great article "[7]The Return of the Web Mob" you can find more details on the

topic as well, such as :

*" I saw one case where an undetectable Trojan was offered for sale and the buyers were debating whether it*

*was worth the price. They were doing competitive testing to ensure it actually worked as advertised," said Jim*

282

*Melnick, a member of Dunham's team. "*

*" In November 2005, Mashevsky discovered an attempt to hijack a botnet. [The] network of infected comput-*

*ers changed hands three times in one day. Criminals have realized that it is much simpler to obtain already-infected resources than to maintain their own botnets, or to spend money on buying parts of botnets which are already in*

*use," he said."*

*" Dunham, who frequently briefs upper levels of federal cyber-security authorities on emerging threats, said*

*there have been cases in Russia where mafia-style physical torture has been used to recruit hackers. If you become a known hacker and you start to cut into their profits, they'll come to your house, take you away and beat you to a pulp until you back off or join them. There have been documented cases of this," Dunham said. "*

While doing a recent research across the Russian and the Chinese domain, I came to the conclusion that ev-

ery local scene has it's own underground, and that those that go as publicly as some do at the bottom line, make the

headlines. However, Chinese users being [8]collectivists, are still at the heroic stage of cyber dissidents slowly turning into wannabe hackers, and they have a chain of command, so to speak, that I can argue is more powerful than

thought to be "well organized" like the ones in Russia, being [9]individualists. There are even marketing campaigns going on in the form of surveys, trying to measure the bargaining point for [10]0day vulnerabilities I guess. This one

says :

**How much would you be willing to pay for an exploit?**

\$100-300

\$300-500

\$500-1000

over \$1000

we write our own exploits :D

I get them for free

283

and offers trying to even add value to the purchase by offering a SMS flooder for free if you purchase the exploit. I mean, if you start thinking logically, bypassing the current intermediaries and their moody programs

compared to one-to-one communication model with a possible buyer – the entire idea behind [11]disintermediation

is the method of choice. Have 0days turned into an uncontrolled commodity that has to be somehow, at least, coordinated?!

In my recent [12]Future trends of malware research, I mentioned how open-source malware would inevitably dominate, and how the concept will put even more pressure on AV vendors to figure out how to protect from unknown malicious code – proactively. What I came across to was, customer-centric malware propositions, special features increase or decrease the final price, botnet sources for free download/purchase if modifications are made, free advices coming with the purchase, on demand vulnerabilities, spamming or spam harvesting services on demand, price comparison for malware samples, [13]rootkits-enabled pieces of malware indeed show an increase of growth, DDoS on demand services are usually proposed with 30 mins of service "demo". Bot's sources are also annoyingly available at the click of a button, as I verified over 20 working links with archives averaging 75MB.

Popular ones :

*urxbot, spybot, sdbot, rxbot, rbot, phatbot, litmus, gtbot, forbot, evilbot, darkirc, agobot, jbot, microbot, blueyebot, icebot, q8bot, happybot, htmlinfectbot, gsys, epicbot, darkbot, r00fuz, panicattack*

284

Who's to blame? It's not Russia for sure, and if it was it would mostly have to do with enforcement of current laws,

yet the global media tends to stereotype to efficiently meet deadlines, instead of figuring out what is going on

at the bottom line. When the U.S sees attacks coming from Chinese networks, it doesn't mean it's Chinese hackers

attacking the U.S, but could be that sick North Korean ones are trying to increase tensions by [14]spoofing their

identities. Moreover, as I've mentioned it is logical to conclude that there are "undergrounds" on a national level, for instance for the last couple of years there's been a steady growth of defacements and phishing attackers from Brazil,

Turkey, and of course China, I rarely come across anything else but "mention Russia and get over it" attitude.

In respect to the Chinese "underground", according a report not to be disclosed, and so I'm not as it's fully

loaded with impressive information, the Chinese underground back in 2002 used to aggressively attack U.S govern-

ment's and military targets while drinking Coke from McDonald's themed Coke glass :) courtesy of the [15]China

Eagle Union themselves. Their [16]actions in coordination with the [17]Honker Union of China, for instance, played a

crucial role in active hacktivism and continue playing it even today.

Like it or not, the average script kiddie, or can we say sophisticated Generation Y teenagers, are well too in-

formed, and obviously sellers of malicious services such as DDoS and malware on demand, than it used to be years

ago. I feel it's not their knowledge that's increasing, but the number of connected computers with security illiterate

users aiming to put themselves in a "stealth mode" while online in order not to get hacked, or as a friend put it, running in root mode and hiding behind firewalls - ah, the end user.

You can [18]digitally fingerprint a malicious code when you have it, that's normal, but what happens when

you don't, can you fight the concepts themselves? Ken Dunham comments on " *mafia-style physical torture*" are the reflection of people naming their malware MyDoom and begging for botnets if you take your time to go through the quotes from [19]Ancheta's [20]case.

285

Don't ph34r the teenagers, ph34r their immaturity, and ongoing recruitment practices by the [21]Mafia itself.

1. [http://www.businessweek.com/magazine/content/05\\_22/b3935001\\_mz001.htm](http://www.businessweek.com/magazine/content/05_22/b3935001_mz001.htm)
2. <http://ddanchev.blogspot.com/2006/03/wheres-my-0day-please.html>
3. <http://www.eweek.com/article2/0,1759,1942497,00.asp?kc=EWRSS03119TX1K0000594>
4. [http://www.theregister.co.uk/2006/03/27/spyware\\_diy/](http://www.theregister.co.uk/2006/03/27/spyware_diy/)

5. <http://www.websensesecuritylabs.com/alerts/alert.php?AlertID=472>
6. <http://www.opera.com/download/index.dml?custom=yes>
7. <http://www.eweek.com/article2/0,1895,1947561,00.asp>
8. <http://en.wikipedia.org/wiki/Collectivism>
9. <http://en.wikipedia.org/wiki/Individualism>
10. <http://ddanchev.blogspot.com/2005/12/0bay-how-realistic-is-market-for.html>
11. <http://en.wikipedia.org/wiki/Disintermediation>
12. <http://www.packetstormsecurity.org/papers/general/malware-trends.pdf>
13. [http://news.com.com/Rootkit+numbers+rocketing+up,+McAfee+says/2100-7349\\_3-6061878.html](http://news.com.com/Rootkit+numbers+rocketing+up,+McAfee+says/2100-7349_3-6061878.html)
14. <http://ddanchev.blogspot.com/2005/12/ip-cloaking-and-competitive.html>
15. <http://www.interfax.cn/showfeature.asp?aid=9724>
16. <http://ddanchev.blogspot.com/2006/02/hacktivism-tensions.html>
17. <http://66.249.93.104/search?q=cache:D58M1Xqr7Ksj:www.cnhonker.com/+Honker+Union+of+China&hl=en&amp;amp;p;amp;amp;amp;amp;ct=clnk&cd=1>



18. <http://ddanchev.blogspot.com/2006/01/why-relying-on-virus-signatures-simply.html>

19. [http://www.usatoday.com/tech/news/computersecurity/infotheft/2006-04-23-bot-herders\\_x.htm](http://www.usatoday.com/tech/news/computersecurity/infotheft/2006-04-23-bot-herders_x.htm)

20. <http://news.findlaw.com/hdocs/docs/cyberlaw/usanchetaind.pdf>

21. <http://en.wikipedia.org/wiki/Mafia>

286

### **In between the lines of personal and sensitive information (2006-04-26 09:52)**

[1]In a previous post, "[2]Give it back!" I mentioned the ongoing re-classification of declassified [3]information and featured some publicly known sources for information on government secrecy. Today I came across to a news item

relating to the topic in another way, "[4]States Removing Personal Data from Official Web Sites", more from the article :

*" At least six states use redaction software, which digitally erases information. It can be tailored to excise nine-digit entries such as SSNs. Chips Shore, circuit court clerk for Florida's Manatee County, removed SSNs and bank*

*account numbers from 3 million public records on the Web site. Another 2.5 million court records were redacted*

*before going online. "*

That's an interesting way to fight the problem from the top of it, namely [5]personal data security breaches

that [6]never stop growing, but I wish they came up with the practice either [7]by default years ago, or understand

today's dynamics of the threat. Even if they start implementing this on a wide scale, it doesn't mean [8]identity theft

would stop occurring, or that [9]phishing attacks wouldn't trick them into giving the complete details. Having imple-

mented a process for securely storing, accessing and trasfering such sensitive customers' bank data, often results

in complexities, but using "redaction software" when you can actually take advantage of a [10]risk management

solution, isn't the smartest move here - yet again that's the effect of today's dynamics and ever-changing attack

vectors. What's the point of putting so much efforts into sanitizing the data before going online with it, when an

outsourcer, or an employee whose responsibilities include working with it will somehow expose it?

Wait, forgot the naive customer who's still taking all the phishing emails received "personally".

Don't think

SSNs and bank accounts "redaction", but insiders and storage/database security.

In respect to removing sensitive information from the Web, I feel the inability of successfully classifying infor-

mation and balancing the accountability in front of society to a certain extent, generates contradictory responses. If

you try to take down a document that has been somehow listed on the Internet or available in digital format, what

you're doing is actually inspiring people to disseminate it, that include news agencies as well, so make sure it doesn't appear there at the first place. Recent cases such as these :

"[11]DOD removes missile defense system report from Web site"

"[12]NORAD orders Web deletion of transcript"

"[13]Air Force One data removed from Web Site revealed details of security measures on president's jets"

"[14]Leaks of Military Files Resume"

bring more insights on the issue.

It is well known that the entire Chinese information warfare doctrine is

backed up by the NCW visions of U.S's military - they still have [15]Sun Tzu's legacy though - and that Al Qaeda's

manuals actually quote U.S military's documents. If you know what exactly you're looking for, you will find it one

way or another, just make sure information-sharing doesn't end up as an information leakage event.

287

Going beyond achieving the balance between usability, accountability, and secrecy, I also feel that disinformation

and deception are reasonably taking place as well, given the reader is actually identified and consequently influenced.

1. <http://photos1.blogger.com/blogger/1933/1779/1600/de-classified-government.1.gif>
2. <http://ddanchev.blogspot.com/2006/02/give-it-back.html>
3. [http://en.wikipedia.org/wiki/Classified\\_information](http://en.wikipedia.org/wiki/Classified_information)
4. [http://www.newsfactor.com/story.xhtml?story\\_id=42930](http://www.newsfactor.com/story.xhtml?story_id=42930)
5. <http://ddanchev.blogspot.com/2006/01/personal-data-security-breaches.html>
6. <http://www.privacyrights.org/ar/ChronDataBreaches.htm>

7. <http://ddanchev.blogspot.com/2006/03/are-cyber-criminals-or-bureaucrats.html>
8. <http://www.bos.frb.org/consumer/identity/idtheft.htm>
9. <http://ddanchev.blogspot.com/2006/04/heading-in-opposite-direction.html>
10. <http://ddanchev.blogspot.com/2005/12/insiders-insights-trends-and-possible.html>
11. <http://www.fcw.com/article92668-03-20-06-Web>
12. [http://news.zdnet.com/2100-9595\\_22-6048254.html](http://news.zdnet.com/2100-9595_22-6048254.html)
13. <http://www.sfgate.com/cgi-bin/article.cgi?file=/c/a/2006/04/11/MNGK3I7A641.DTL>
14. <http://www.latimes.com/news/nationworld/world/la-fg-drives25apr25,0,1174262.story?track=tohtml>
15. <http://www.kimsoft.com/polwar.htm>

288

## **DIY Marketing Culture (2006-04-27 13:16)**

**Problem** - big name advertising agencies, and self forgotten copywriters easily turn into an obstacle for a newly

born startup, the way marketing researchers can easily base your entire service/product development efforts on

a single survey's results. Generating content, thinking content is the king, trying to sense and understand your

customers' needs or where the market is heading to for the sake of responding with profitable propositions, I think

is a self-centered, in-the-box mode of thinking that would cease to exist with customers becoming more informed.

**Solution** - Don't get too "product-concept" centered, instead solve a problem profitably and retain their satisfaction for as long as possible. Let your customers dictate the rules, and perhaps even generate your entire marketing

promotional efforts themselves - literally. Did you know you could get yourself [1]custom printed MM's? I recently

found out I can, and I'm already expecting the packs.

Or how the successfully positioned as a secure alternative to IE, FireFox browser actually invested pennies in

[2]spreading the word about it? Moreover, a \$5000 bounty can indeed promote creativity, given they are comfort-

able with the idea, and with the 280 user-generated ads generated at [3]FireFox Flicks I think they did it again, no

wait, their users did it. Take your time to go through the flicks, it's worthwhile.

Question the concepts, rethink them, and disrupt with whatever the outcome.

1. <http://www.mymms.com/customprint/index.asp>

2. <http://www.spreadfirefox.com/>

3. <http://www.firefoxflicks.com/flicks/>

## **A comparison of US and European Privacy Practices (2006-04-27 14:27)**

[1][2]A new study on "[3]US and European Corporate Privacy Practices" was [4]released two days ago, and as I

constantly monitor the topic knowing EU's stricter information sharing and privacy violations laws comparing to the

U.S, thought you might find this useful. To sum up the findings :

*" European companies are much more likely to have privacy practices that restrict or limit the sharing of cus-*

*tomer or employees' sensitive personal information and are also more likely to provide employees with choice or*

*consent on how information is used or shared," said David Bender, head of White & Case's Global Privacy practice. "*

still at the "sharing sensitive information is bad"

promotional stage, I feel the research reasonable points out the lack of a systematic technical approach, [5]bureau-

cracy can also be an issue, but with so many [6]CERTs in Europe there's potential for lots of developments I think.

Established in 2004, [7]ENISA is the current body overseeing and guiding the Community towards data protection

practices – slowly, but steadily gaining grounds.

*" But the research also revealed that US companies are engaging in more security and control-oriented compli-*

*ance activities than their European counterparts. As a result, US corporations scored higher in five of the eight areas of corporate privacy practice. " - structured implementation on a technical level, that is people auditing networks and being accountable in case of not doing so, and privacy policies by default. A little something bringing more insight*

from the [8]Safe Harbor framework :

*" The United States uses a sectoral approach that relies on a mix of legislation, regulation, and self regulation.*

*The European Union, however, relies on comprehensive legislation that, for example, requires creation of government*

*data protection agencies, registration of data bases with those agencies, and in some instances prior approval before personal data processing may begin. "*

Of course there are differences and there should always be as they provoke constructive discussions, but among the

many well-developed survey questions, some made me a quick impression :

*" Is there a process for communicating the privacy policy to all customers and consumers? " Europe - 33 % United States - 69 %*

*" Is privacy training mandatory for key employees (those who handle, manage or control personal information)? "*

Europe - 22 % United States - 62 %



*" Do you use technologies to prevent unauthorized or illegal movement or transfer of data or documents? "* Europe - 17 % Unites States - 45 %

*" Will the company notify individuals when their personal information is lost or stolen? "* Europe 33 % United States - 62 %

Perimeter based defenses naturally dominate as a perception of being secure, still, I feel that the growing infosec

market and IT infrastructures in both the U.S and Europe would continue to fuel the growth of new technologies

and also result in more informed decision makers – at the bottom line it's always about a common goal and better

information sharing.

1. <http://photos1.blogger.com/blogger/1933/1779/1600/no-more-invasions.1.jpg>

2. [http://photos1.blogger.com/blogger/1933/1779/1600/Europe\\_CERTs.jpg](http://photos1.blogger.com/blogger/1933/1779/1600/Europe_CERTs.jpg)

3. <http://www.whitecase.com/news/Detail.aspx?news=1091>

4. <http://www.whitecase.com/files/Publication/1e7a69e0-49e9-478e-abc1-303e107c4dd7/Presentation/PublicationAttachment/4a78432a-bd1f-4363-ab82-32fab1729a1e/Benchmark>

5. <http://ddanchev.blogspot.com/2006/03/are-cyber-criminals-or-bureaucrats.html>

6.

[http://www.enisa.eu.int/doc/pdf/deliverables/enisa\\_cert\\_euro\\_map\\_v1\\_2060210.pdf](http://www.enisa.eu.int/doc/pdf/deliverables/enisa_cert_euro_map_v1_2060210.pdf)

7. <http://www.enisa.eu.int/>

8. <http://www.export.gov/safeHarbor/index.html>

291

**2.5**

**May**

292

### **April's Security Streams (2006-05-02 11:39)**

[1]Hi folks, it's about time to quickly summarize April's Security Streams. As of today, my blog is officially six months old and the feeling of witnessing change and improvements has always been a pleasant one. Blogging "my way"

takes a lot of time, that is, posts going beyond "preaching" but emphasizing on "teaching", a little bit of investigative research, full-disclosure, and constructive key points on emerging or possible future trends related to infosec. Thanks

for everyone's feedback, and actually reading not just going my posts as far as the average visitors' time spent is

concerned!

**1.** "[2]Wanna get yourself a portable Enigma encryption machine?"Already sold, but auctioned on Ebay, it's remarkable how the seller managed to preserve an original Enigma in such a condition, and the bids were worth it!

**2.** "[3]The "threat" by Google Earth has just vanished in the air" Coming across Microsoft's [4]Windows Live Local Street-Side Drive-by provoked contradictory thoughts, so I've decided to sum up recent ideas on the issue. The

[5]use of public satellite imagery for conducting OSINT is inevitable, while on the other hand the providers are simply

making the world a smaller place. It is also questionable whether potential terrorists are "abroad" or within the countries themselves, that is knowing each and every corner of a possible "attack location", but with the ability to syndicate and share maps it would be naive not to think that they way you chat, they also do, and the way you plan

activities while "zooming-out", they also do. At the bottom line, snooping from above might actually deal more with self-confidence than anything else. Have an opinion? Feel free to comment on the topic

**3.** "[6]Insider fined \$870" [7]Virtual worlds are emerging and so are security techniques to steal someone's sword, be it through insiders, phishing, or trojan horse attacks. What's important to keep in mind when it comes to

insiders is that on the majority of occasions you're are never aware that there's an ongoing potential breach on its

way, and moreover, that the quantitative losses due to insiders are totally based on a company's sales projections,

rather than successfully (if one can) measuring the value of intellectual property

**4.** "[8]Securing political investments through censorship" We constantly talk on how the Internet is changing our daily

lives, our attitudes, and giving us the opportunity to tap into the biggest think-tank in the world – on the

majority of occasions for free. Internet censorship is still a very active practice by well-known regimes, while this

post was trying to emphasize on the current situation – securing political investments through censorship

**5.** "[9]Heading in the opposite direction" Companies and financial institutions are the most often targets of phishing attacks, and it's getting hard for them to both, convince their users and society that they're working on

fighting the problem, and most importantly where's the real problem and how to fight it. In this post, I try to

emphasize that building communications over a broken channel Bank2Customer over email is the worst possible

strategy you could start executing. The irony in here is how in the way both, phishers and any bank in question may

sometimes be using images stored on the banks server – altogether!

293

**6.** "[10]IM me" a strike order" It's a common myth that the military have come up with a Über secret and secure communications network, going beyond the Internet. And while there're such, they all suffer the same

weakness, lack of usability, and budget deficits compared to IP based communications, that is the Internet. The post

goes through research surveys on IMs in the military, and tries to bring more awareness on how age-old IM threats

can easily exploit military IM communications as well

**7.** "[11]Catching up on how to lawfully intercept in the digital era" On as daily basis we discuss security breaches, threats, privacy violations, whereas constantly misses the fact that there's a practice called lawful interception,

namely that even if the NSA's domestic spying program got so much attention and concerns, it doesn't mean they

aren't going to continue keeping themselves up-to-date with what is going wherever OSINT, SIGINT and HUMINT are

applicable. The bottom line is that a person behind a CCTV camera's network is also under surveillance, so I advise

you go through a very good resource on the topic, the [12]Surveillance and Society Journal

**8.** "[13]On the Insecurities of the Internet" IP spoofing by default, DNS and BGP abuses, Distributed Reflection Denial of Service Attacks, are among the ones worth mentioning, while perhaps the biggest insecurity lies in

the fact that the Internet we're all striving to adapt for E-commerce and E-business, was developed as a scientific

network we got used to so fast

**9.** "[14]Distributed cracking of a utopian mystery code" Continuing the "distributed concepts" series of posts, this one deals with virtual worlds, and a wise idea on how to keep the players coming back for more - let them even

bruteforce the next part of the puzzle

**10.** "[15]Fighting Internet's email junk through licensing"  
China's Internet population is about to surpass the U.S one  
and it would continue to grow resulting in China becoming  
the "novice" king of insecure networks. Trying to centrally  
control spam, they you can control the flow of traffic going  
out and coming in the country is a typical,

but weak approach that could have worked years ago as no  
one needs a mail server to generate spam or phishing

attacks these days. In respect to their concerns of users  
learning more about infosec, in China a cyber dissident is a

heroic potential hacker, one that can easily bypass the Great  
Firewall and spread the word on how it can be done.

As a matter of fact, PBS has done an outstanding job in their  
[16]Tank Man episode, and while many considered

the Chinese students' inability to recognize the  
[17]infamous photo, what they were actually afraid of is  
showing a

face-gesture that they indeed recognized it - as they did of  
course.

**11.** "[18]Would somebody please buy this Titan 1 ICBM  
Missile Base?" I think the buyer of this base should have  
better thought of what he's buying, or let's just say how on  
Earth was he expecting to break-even given he missed

the post-cold war momentum itself? It's indeed once in a  
lifetime purchase that you would think twice before not

purchasing, and so I hope the auction would continue to attract visitors the way it is – high-profit margins whenever the momentum is lost is a "lost case" by itself

294

**12.** "[19]Spotting valuable investments in the information security market" An in-depth post on current market and vendor trends, as well as more info on the, now fully realistic acquisition of SiteAdvisor my McAfee,

something I've blogged about in [20]January. It's great to know that both parties came across the posts themselves,

and to witness how such a wide-scale community power, but still backed by technology, startup got so easily acquired.

What the acquirer must now ensure, is that it doesn't cannibalize the culture at SiteAdvisor – every day is a startup

day for us type of attitude is a permanent generator of creativity and attitude

**13.** "[21]Digital forensics - efficient data acquisition devices" A resourceful post mentioning on the release of the CellIDEK, no, it's not a portable DJs one, but a acquisition device detecting over 160 cell phone models and having

the capacity to simultaneously acquire it from numerous devices all at once. Virtual cyber crime is all about quality

forensics, whereas different legislations and approaches for gathering and coordinating such data across various

countries remains a problem

**14.** "[22]The anti virus industry's panacea - a virus recovery button" Try to get this on the Super Bowl and watch a generating falling for the lack of complexity in this "solution". Gratefully, I got many comments from readers with cheers on mentioning this and how useless the button is at the bottom line

**15.** "[23]Why's that radar screen not blinking over there?" Quite some [24]sites picked up the story, yet we can always question, and than again, so what? In a crucial situation a scenario like this could prove invaluable for the final outcome, but right now it's just a PR activity from the other side of the camp. Symmetric warfare is a tangible

defense/offensive concept, whereas asymmetric warfare is fully capable of balancing powers - to a certain extend as

no matter how much NCW you put on the ground, you would still need "tangible" forces on the finish line

**16.** "[25]25 ways to distinguish yourself - and be happy?" A little bit of self-esteem is never too much and that's what these series can help you with

**17.** "[26]Wild Wild Underground" An in-depth summary of some findings I intended to post for quite some

time, but didn't have the time to. If you just take yourself some time to rethink over, you would hopefully realize

that a [27]guy like this is capable of recruiting people who actually come up with their own algorithms - beyond their

will in one way or another. Moreover, responding to comments I received, of course I did report the links, which are



now down, as well as some of the forum posts I managed to digg. Ryan1918 is rather active though

**18.** "[28]In between the lines of personal and sensitive information" Government reclassification of documents isn't the most pragmatic way, as these have already been online once, therefore someone out there still keeps a copy, and

is now more than ever motivated to disseminate it, given someone is trying to censor it. I feel a common structure

of the different types of information, formal training for those dealing with that type of info etc. and putting in place risk management solutions, considering that humans are totally not to be trusted (are computers to be?) is a way

295

to mitigate these risks. Trying to censor something you end up making it even more popular that it could have been without you censoring it, just a thought

**19.** "[29]DIY Marketing Culture" Personalization and Customization are emerging by default, and so is virtual viral marketing. In this post I mention the possibility to get your own custom MMs, and FireFox's FireFlicks initiative

**20.**

"[30]A comparison of US and European Privacy Practices" You can rarely come across a infosec survey

with well formulated questions, ones that are the basis of a quality one. I think this company did a very good job in

formulating and summarizing the outcome of a very trendy topic

[31][32]

Updated to add the averages for each month since I've started tracking my readers, looks nice, and in case

you're interested you can also go [33]through the [34]summaries of [35]previous months.

1.

[http://photos1.blogger.com/blogger/1933/1779/1600/Mind%20blowing\\_Nicholas%20Cann.9.jpg](http://photos1.blogger.com/blogger/1933/1779/1600/Mind%20blowing_Nicholas%20Cann.9.jpg)

2. <http://ddanchev.blogspot.com/2006/04/wanna-get-yourself-portable-enigma.html>

3. <http://ddanchev.blogspot.com/2006/04/threat-by-google-earth-has-just.html>

4. <http://preview.local.live.com/>

5.

<http://maps.google.com/maps?q=yakima,+wa&t=k&am;am;am;am;am;am;am;am;am;am;hl=e>

[n&ll=46.682193,-120.356877&spn=0.006801,0.019913&om=1](http://maps.google.com/maps?q=yakima,+wa&t=k&am;am;am;am;am;am;am;am;am;am;hl=en&ll=46.682193,-120.356877&spn=0.006801,0.019913&om=1)

6. <http://ddanchev.blogspot.com/2006/04/insider-fined-870.html>

7. <http://virtualworldsreview.com/>

8. <http://ddanchev.blogspot.com/2006/04/securing-political-investments-through.html>

9. <http://ddanchev.blogspot.com/2006/04/heading-in-opposite-direction.html>
10. <http://ddanchev.blogspot.com/2006/04/im-me-strike-order.html>
11. [http://ddanchev.blogspot.com/2006/04/catching-up-on-how-to-lawfully\\_12.html](http://ddanchev.blogspot.com/2006/04/catching-up-on-how-to-lawfully_12.html)
12. <http://www.surveillance-and-society.org/>
13. [http://ddanchev.blogspot.com/2006/04/on-insecurities-of-internet\\_13.html](http://ddanchev.blogspot.com/2006/04/on-insecurities-of-internet_13.html)
14. <http://ddanchev.blogspot.com/2006/04/distributed-cracking-of-utopian.html>
15. <http://ddanchev.blogspot.com/2006/04/fighting-internets-email-junk-through.html>
16. <http://www.pbs.org/wgbh/pages/frontline/tankman/>
17. <http://ddanchev.blogspot.com/2006/01/twisted-reality.html>
18. <http://ddanchev.blogspot.com/2006/04/would-somebody-please-buy-this-titan-1.html>
19. <http://ddanchev.blogspot.com/2006/04/spotting-valuable-investments-in.html>
20. <http://ddanchev.blogspot.com/2006/02/look-whos-gonna-cash-for-evaluating.html>
21. <http://ddanchev.blogspot.com/2006/04/digital-forensics-efficient-data.html>

22. <http://ddanchev.blogspot.com/2006/04/anti-virus-industrys-panacea-virus.html>
23. <http://ddanchev.blogspot.com/2006/04/whys-that-radar-screen-not-blinking.html>
24. <http://www.google.com/search?hl=en&lr=&q=%22Russian+bombers+flew+undetected+across+Arctic%22&btnG=Search>
25. <http://ddanchev.blogspot.com/2006/04/25-ways-to-distinguish-yourself-and-be.html>
26. [http://ddanchev.blogspot.com/2006/04/wild-wild-underground\\_25.html](http://ddanchev.blogspot.com/2006/04/wild-wild-underground_25.html)
27. [http://dsc.discovery.com/news/briefs/20060417/mafiaboss\\_tec.html](http://dsc.discovery.com/news/briefs/20060417/mafiaboss_tec.html)
28. <http://ddanchev.blogspot.com/2006/04/in-between-lines-of-personal-and.html>
29. <http://ddanchev.blogspot.com/2006/04/diy-marketing-culture.html>
30. <http://ddanchev.blogspot.com/2006/04/comparison-of-us-and-european-privacy.html>
- 296
31. [http://photos1.blogger.com/blogger/1933/1779/1600/April\\_Streams\\_Stats.0.jpg](http://photos1.blogger.com/blogger/1933/1779/1600/April_Streams_Stats.0.jpg)
32. <http://photos1.blogger.com/blogger/1933/1779/1600/Securi>

[ty\\_Minds\\_Streams.jpg](#)

33. <http://ddanchev.blogspot.com/2006/01/januarys-security-streams.html>

34. <http://ddanchev.blogspot.com/2006/03/februarys-security-streams.html>

35. <http://ddanchev.blogspot.com/2006/03/marchs-security-streams.html>

297

### **Biased Privacy Violation (2006-05-03 13:37)**

[1]This is a very interesting initiative, going beyond the usual [2]MySpace's teen heaven [3]privacy issues, but directly exposing the mature audience in a way I find as a totally biased one. Girls writing stories on men that supposedly

chated on them. [4]DontDateHimGirl.com aims to :

*" DontDateHimGirl.com is an online resource for women who have shared the experience of dating a no-good*

*man! Browse our search engine of alleged cheaters, liars and cads right now! This controversial site has been*

*featured on MSNBC, the Today Show, ABC News, CNN and Entertainment Tonight! There is finally a way for women*

*to check a guy out BEFORE dating, marrying or otherwise committing to him! Warn other women about the men who*

*have cheated, lied or used you! Register and become a member today! You'll receive our free newsletter and other*

*valuable goodies! It's fast, easy and best of all, it's free! You'll be doing your sisters around the world an invaluable service! Don't Date Him Girl! "*

Basically stuff like, "post a cheating man", "[5]search for a cheating man", or browse through the 3593 ones already "categorized" as cheaters with personal stories and photos whenever available. What I feel they shouldn't do, is aggregate that kind of community powered personal details for third-parties, and making it searchable. Some

stories are pretty fun and average enough to make you think :

*" Quite a charmer in the beginning, as all guys tend to be. Called me beautiful, gorgeous.. kissed my fore-*

*head.. He did all the right things. He could do no wrong. We "dated" for a good 6 months, and things seemed to be going good. He was the love of my life. Lots of firsts with him, then he did a total 180. He stopped calling and didn't respond to my phone calls and/or messages. I was so distraught. I thought I did something to fuck things up. "*

Perhaps she did, didn't she?! Still, that's entirely between them given they actually respect each other.

Don't get me wrong, there are pathological polygamists, but what's next, Local Google Maps to pin point the

cheating areas around town?

To balance the powers, and make it even worse there's even a [6]DontDateHerMan.com coming along, but try

not to bring your **personal life** stuff to such an end, or is it just me? :)

1. <http://photos1.blogger.com/blogger/1933/1779/1600/dont-date-him.2.jpg>
2. [http://www.forbes.com/columnists/2006/04/25/myspace-kids-protection-cx\\_cw\\_0425myspace.html](http://www.forbes.com/columnists/2006/04/25/myspace-kids-protection-cx_cw_0425myspace.html)
3. <http://ddanchev.blogspot.com/2006/03/future-of-privacy-dont-over-empower.html>
4. <http://www.dontdatehimgirl.com/>
5. <http://dontdatehimgirl.com/search/>
6. <http://dontdateherman.com/>

298

### **Travel Without Moving - Typhoon Class Submarines (2006-05-04 13:50)**

[1]In previous posts "[2]Security quotes : a FSB (successor to the KGB) analyst on Google Earth", "[3]Suri Pluma - a satellite image processing tool and visualizer", "[4]The "threat" by Google Earth has just vanished in the air" I talked about various issues related to satellite imagery and security.

Moreover, I'm also actively covering various emerging [5]Space Warfare issues, and with the recent specula-

tion that the [6]Okno ELINT complex in Tajikistan is becoming Russian and different "schools of thought", there's a lot to come for sure. Google Maps/Earth did not only [7]restart the real estate industry, it made the world a smaller

place, a more [8]competitive one, and hopefully a safer one if security counts here.

As of today, I decided to start posting a weekly section, the "**Travel Without Moving**" series, presenting interesting and publicly obtained imagery of sights that somehow made me an impression. The other day I came across

to a (perhaps scraped by now) [9]Typhoon Class Submarines at [10]GoogleSightseeing.com – the largest and quietest types of submarines.

That's perhaps the perfect moment to mention the cool pictures of a [11]Soviet Underground Submarine Base

in the Nuclear Submarine Base that "*Until the collapse of the Soviet Union in 1991 Balaklava was one of the most secret towns in Russia. 10km south eas of Sevastopol on the Black Sea Coast, this small town was the home to a*

*Nuclear Submarine Base.*" Take a tour for yourself!

1.  
[http://photos1.blogger.com/blogger/1933/1779/1600/Typhoon\\_Class\\_Submarines.jpg](http://photos1.blogger.com/blogger/1933/1779/1600/Typhoon_Class_Submarines.jpg)
2. <http://ddanchev.blogspot.com/2006/01/security-quotes-fsb-successor-to-kgb.html>
3. <http://ddanchev.blogspot.com/2006/02/suri-pluma-satellite-image-processing.html>
4. <http://ddanchev.blogspot.com/2006/04/threat-by-google-earth-has-just.html>



5. <http://ddanchev.blogspot.com/2006/04/threat-by-google-earth-has-just.html>
6. <http://enews.ferghana.ru/detail.php?id=95267645613.42,338,11358995>
7. <http://www.housingmaps.com/>
8. <http://local.live.com/>
9. [http://en.wikipedia.org/wiki/Typhoon\\_class\\_submarine](http://en.wikipedia.org/wiki/Typhoon_class_submarine)
10. <http://googlesightseeing.com/maps?p=&c=&amp;amp;t=k&hl=en&ll=69.434275,32.355123&z=15>
11. <http://www.funmansion.com/html/fm-Soviet-Underground-Submarine-Base.html>

299

## **The Current State of Web Application Worms (2006-05-04 14:50)**

[1]Remember the most [2]recent [3]Yahoo! Mail's XSS vulnerabilities, or the [4]MySpace worm? I just read through a

well written summary on Web Application Worms by [5]Jeremiah Grossman, from WhiteHat Security, "[6]Cross-Site

Scripting Worms and Viruses - The Impending Threat and the Best Defense", an excerpt :

*" Samy, the author of the worm, was on a mission to be famous, and as such the payload was relatively be-*

*nign. But consider what he might have done with control of over one million Web browsers and the gigabits of*

*bandwidth at their disposal—browsers that were also potentially logged-in to Google, Yahoo, Microsoft Passport,*

*eBay, web banks, stock brokerages, blogs, message boards, or any other web-based applications. It's critical that we begin to understand the magnitude of the risk associated with XSS malware and the ways that companies can defend*

*themselves and their users. Especially when the malware originates from trusted websites and aggressive authors. In*

*this white paper we will provide an overview of XSS; define XSS worms; and examine propagation methods, infection*

*rates, and potential impact. Most importantly, we will outline immediate steps enterprises can take to defend their websites. "*

It provides an overview of Cross-Site Scripting (XSS), Methods of Propagation, comments on the First XSS Worm,

a worst case scenario, and of course protection methods, nice graphs and overview of this emerging trend. In my

"[7]Future Trends of Malware" research I indeed pointed out on its emergence :

*" How would a malware author be able to harness the power of the trust established between, let's say, [8]ComScore's top 10 sites and their visitors? Content spoofing is the where the danger comes from in my opinion, and obvious web*

*application vulnerabilities, or any bugs whose malicious payload could be exposed to their audiences. In case you*

*reckon, a nasty content spoofing on Yahoo!'s portal resulted in the following possibility for driving millions of people at a certain URL, if I don't trust what I see on Yahoo.com or Google.com, why bother using the Net at all is a common mass attitude of course. Any web property attracting a relatively large number of visitors should be considered as a propagation vector, for both, malware authors, and others such as phishers, or botnet brokers for instance. "*

[9]

[10]Monetizing [11]mobile malware is among the other trends I also indicated, and the [12]RedBrowser seems to be

the most recent example of this as it randomly chooses a premium-rate number from the following list, and sends

a SMS message generating revenue for the attacker :

*08293538938, 08001738938, 08180238938, 08229238938,*

*08441238938, 08287038938, 08187938938, 08189038938, 08217838938, 08446838938.*

I summarized the key points back than as :

*" The number and penetration of mobile devices greatly outpaces that of the PCs.*

*Malware authors are ac-*

*tively experimenting and of course, progressing with their research on mobile malware. The growing monetization of*

*mobile devices, that is generating revenues out of users and their veto power on certain occasions, would result in*

*more development in this area by malicious authors. SPIM would also emerge with authors adapting their malware*

*for gathering numbers. Mobile malware is also starting to carry malicious payload. Building awareness on the the*

300

*issue, given the research already done by several vendors, would be a wise idea. "*

Among the first folks to discuss the topic of web application malware was Robert from CGISecurity.com in his

"[13]Anatomy of Web Application Worm" paper back in 2002, and with the ease and speed of discovering web

application vulnerabilities in major portals it's up to the imagination of the attacker - as the paper points out Samy

only wanted to make 1 million friends, what if he wanted to do something else?

[14]

"[15]Cross-Site Scripting Worms and Viruses - The Impending Threat and the Best Defense" also argues on

Samy being the fastest worm, though single-packet UDP worms, according to a research on the "[16]Top Speed of

Flash Worm" by " *Simulating a flash version of Slammer, calibrated by current Internet latency measurements and observed worm packet delivery rates, we show that a worm could saturate 95 % of one million vulnerable hosts on*

*the Internet in 510 milliseconds. A similar worm using a TCP based service could 95 % saturate in 1.3 seconds. The*

*speeds above are achieved with flat infection trees and packets sent at line" rates.*

Is it the speed or the size of the infected targeted group that matters, and what if Web 2.0 worms can achieve exactly

the two of these?

More resources on the topic in case you are interested :

[17]Web-based Malware & Honeypots - [18]phpBB bots/worms

[19]New MySpace XSS worm circulating

[20]Description of a Yahoo! Mail XSS vulnerability

[21]Evolution of Web-based worms

[22]The Latest in Internet Attacks: Web Application Worms

[23]Web Application Worms : Myth or Reality?

[24]Analysis of Web Application Worms and Viruses

[25]Paros - for web application security assessment

1. <http://photos1.blogger.com/blogger/1933/1779/1600/y-XSS.jpg>

2. <http://www.securityfocus.com/archive/1/413594/30/0/threaded>

3. [http://www.webappsec.org/projects/whid/list\\_id\\_2006-26.shtml](http://www.webappsec.org/projects/whid/list_id_2006-26.shtml)
4. <http://namb.la/popular/>
5. <http://www.whitehatsec.com/management.html>
6. <http://www.whitehatsec.com/downloads/WHXSSThreats.pdf>
7. <http://packetstormsecurity.org/papers/general/malware-trends.pdf>
8. <http://www.comscore.com/press/release.asp?press=447>
9. <http://photos1.blogger.com/blogger/1933/1779/1600/000000015688.jpg>
10. <http://www.symantec.com/avcenter/venc/data/trojan.redbrowser.a.html>
11. [http://www.informatik.uni-hamburg.de/SVS/personnel/henrich/RiskAnalysis\\_of\\_Mobile\\_Devices\\_with\\_special\\_Concern\\_of\\_Malware\\_Contamination.pdf](http://www.informatik.uni-hamburg.de/SVS/personnel/henrich/RiskAnalysis_of_Mobile_Devices_with_special_Concern_of_Malware_Contamination.pdf)
12. <http://www.f-secure.com/weblog/archives/archive-022006.html#00000823>
13. <http://www.cgisecurity.com/articles/worms.shtml>
14. [http://photos1.blogger.com/blogger/1933/1779/1600/Worm\\_Propagation.jpg](http://photos1.blogger.com/blogger/1933/1779/1600/Worm_Propagation.jpg)

301

15.

<http://www.whitehatsec.com/downloads/WHXSSThreats.pdf>

16. <http://www.icir.org/vern/papers/topspeed-worm04.pdf>

17. <http://honeyblog.org/archives/35-Web-based-Malware-Honeypots.html>

18. <http://isc.sans.org/diary.php?storyid=1275>

19. <http://xavsec.blogspot.com/2005/12/new-myspace-xss-worm-circulating.html>

20. <http://www.packetstormsecurity.org/0604-advisories/yahoo-xss-2.txt>

21. <http://www.securityfocus.com/columnists/364>

22. <http://www.securitypark.co.uk/article.asp?articleid=24240&CategoryID=1>

23. [http://security-protocols.com/whitepapers/Application\\_Worms.pdf](http://security-protocols.com/whitepapers/Application_Worms.pdf)

24.

[http://www.spidynamics.com/spilabs/education/presentation/s/billyhoffman-web\\_appworms\\_viruses.pdf](http://www.spidynamics.com/spilabs/education/presentation/s/billyhoffman-web_appworms_viruses.pdf)

25. <http://www.parosproxy.org/index.shtml>

302

**Shaping the Market for Security Vulnerabilities  
Through Exploit Derivatives (2006-05-08 20:47)**

In a previous post "[1]0bay - how realistic is the market for security vulnerabilities?" I gave a brief overview of the current market intermediaries and their position, listed various research I recommend you to go through, and speculated on an [2]auction based market model.

During April, at the CanSecWest Security Conference "[3]Groups argued over merits of flaw bounties" some quotes :

*" The only economic model that does not make sense to me is the vendor's," Sutton said. "They get to know about a vulnerabilities ahead of time, but they are unwilling to pay for them. " - Michael Sutton*

*" What I can give people who find vulnerabilities is a small amount of fame. iDefense can give them \$10,000. "*

*- Darius Wiles*

*" As a civil rights issue, selling vulnerabilities is just fine.*

*As a keeping-the-customers safe issue, it's junk. " -*

Novell director of software engineering Crispin

*" If I come to you and offer to sell you a vulnerability in your product, I am going to be cuffed and arrested,"*

*he told the representatives of software makers on the panel.*  
*" - Matthew Murphy*

And the discussion is reasonably pretty hot with a reason. Back in January [4]Microsoft expressed their opin-

ion on the intermediaries based market model like :



*" One day after iDefense, of Reston, Va., announced the bounty as part of a newly implemented quarterly hack-*

*ing challenge, a spokesperson for Microsoft, based in Redmond, Wash., said paying for flaws is not the best way to*

*secure software products. "We do not believe that offering compensation for vulnerability information is the best way [researchers] can help protect customers," the spokesperson said in a statement sent to eWEEK. "*

and while Microsoft talks about responsible disclosure, that's exactly the type of model I don't really think ex-

ist anymore. [5]Peter Mell made a good point that *" I don't support this activity. Basically, it enables third parties to unfairly focus attention on a particular vendor or product. It does not help security in the industry," Mell said in an interview with eWEEK. "* – but it still offers the opportunity to bring order into the chaos doesn't it?

The [6]WMF vulnerability apparently got purchased for \$4000 and I among the few scenarios that I mentioned

303

were on vendors purchasing vulnerabilities and requested vulnerabilities, or a reverse model :

*" requested vulnerabilities are the worst case scenario I could think of at the moment. Why bother and always*

*get excited about an IE vulnerability, when you know person/company X are running Y AV scanner, use X1 browser*

*as a security through obscurity measure. That's sort of reverse model compared to current one where researchers*

*"push" their findings, what if it turns into a "pull" approach, "I am interested in purchasing vulnerabilities affecting that version of that software", would this become common, and how realistic is it at the bottom line? "*

Coming across [7]0day vulnerabilities for sale, I also came across Rainer Boehme's great [8]research on vari-

ous market models, among them exploit derivatives. Have you ever thought of using exploit [9]derivatives, on the

called "[10]futures market"? I think the idea has lots of potential, and he described it as :

*" Instead of trading sensitive vulnerability information directly, the market mechanism is build around contracts that pay out a defined sum in case of security events. For instance, consider a contract that pays its owner the sum of 100 EUR on say 30 June 2006 if there exists a remote root exploit against a precisely specified version of ssh on a defined platform. "*

The OS/Vendor/Product/Version/Deadline type of reverse model that I also mentioned is a good targeted con-

cept if it were used by vendors for instance, and while it has potential to have a better control over the market, the

lack of common and trusted body to take the responsibility to target [11]Windows and [12]Apple 50/50 for instance,

still makes me think. The best part is how it would motivate researchers at the bottom line - deadlines result in

spontaneous creativity sometimes.

More on the topic of security vulnerabilities and commercializing the market, in a great [13]article by Jennifer

Granick (remember [14]Michael Lynn's case?) [15]she said that :

*" I'm more concerned that commercialization, while it promotes discovery, will interfere with the publication of vulnerability information. The industry adopted responsible disclosure because almost everyone agrees that members of the public need to know if they are secure, and because there is inherent danger in some people having*

*more information than others. Commercialization throws that out the window. Brokers that disclose bugs to their*

*selected list of subscribers are necessarily withholding important information from the rest of the public. Brokers may eventually issue public advisories, but in the meantime, only the vendor and subscribers know about the problem. "*

Who should be empowered at the bottom line, the intermediaries centralizing the process, or the security re-

searchers/vulnerability diggers starting to seek bids for their research efforts?

On the other hand, I think that the current market model suffers from a major weakness and that is the need

for achieving faster liquidity if we can start talking about such.

Basically, sellers of vulnerabilities want to get their commissions as soon as possible, which is where the lucrative underground market easily develops. While I am aware of cases where [16]insurers are already purchasing

vulnerabilities to hedge risks until tomorrow I guess, anyone would put some effort into obtaining a critical MS

vulnerability given a deadline and [17]hefty reward, but who's gonna act as a social planner here?

1. <http://ddanchev.blogspot.com/2005/12/0bay-how-realistic-is-market-for.html>
2. <http://www.cl.cam.ac.uk/~jo262/papers/weis04-ozment-bugauc.pdf>
3. [http://www.theregister.co.uk/2006/04/06/vulnerability\\_purchasing\\_debate/](http://www.theregister.co.uk/2006/04/06/vulnerability_purchasing_debate/)
4. <http://www.eweek.com/article2/0,1895,1928389,00.asp>
5. <http://nvd.nist.gov/>
6. <http://ddanchev.blogspot.com/2006/01/was-wmf-vulnerability-purchased-for.html>
7. <http://ddanchev.blogspot.com/2006/03/wheres-my-0day-please.html>
8. [http://events.ccc.de/congress/2005/fahrplan/attachments/542-Boehme2005\\_22C3\\_VulnerabilityMarkets.pdf](http://events.ccc.de/congress/2005/fahrplan/attachments/542-Boehme2005_22C3_VulnerabilityMarkets.pdf)
9. [http://en.wikipedia.org/wiki/Derivatives\\_market](http://en.wikipedia.org/wiki/Derivatives_market)

10. <http://www.google.com/search?hl=en&lr=&q=define%3Afutures+market>
11. <http://ddanchev.blogspot.com/2006/03/5-things-microsoft-can-do-to-secure.html>
12. <http://ddanchev.blogspot.com/2006/02/one-bite-only-at-least-so-far.html>
13. <http://www.wired.com/news/columns/0,70644-0.html>
14. [http://en.wikipedia.org/wiki/Michael\\_Lynn](http://en.wikipedia.org/wiki/Michael_Lynn)
15. [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=874846](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=874846)
16. [http://ddanchev.blogspot.com/2006/03/getting-paid-for-getting-hacked\\_17.html](http://ddanchev.blogspot.com/2006/03/getting-paid-for-getting-hacked_17.html)
17. <http://ddanchev.blogspot.com/2006/02/how-to-win-10000-bucks-until-end-of.html>

305

### **The Cell-phone Industry and Privacy Advocates VS Cell Phone Tracking (2006-05-09 15:19)**

[1]I've once mentioned various [2]privacy issues related to mobile devices, the growing trend of "assets tracking", and of course, cell phones tracking. Yesterday I came across to great summary of the current situation – privacy

groups make a point of it. From the [3]article :

*" Real-time tracking of cell phones is possible because mobile phones are constantly sending data to cell tow-*

*ers, which allows incoming calls to be routed correctly. The towers record the strength of the signal along with the side of the tower the signal is coming from. This allows the phone's position to be easily triangulated to within a few hundred yards. But the legal grounds for obtaining a tracking order is murky – not surprising since technology often outpaces legislation. The panel agreed that Congress should write rules governing what level of suspicion cops need*

*to have before tracking people through their cell phones."*

While on the other hand, there's also an ongoing commercialization of the [4]service by the industry itself, if

the government were to start using practices like these with grey subpoenas, it would undermine the customers'

trust in the industry and BigBrother is going to get even bigger. Enthusiasts are already [5]experimenting with

DIY cell phone tracking abilities, so if you worry about being tracked through your phone, you should also start

worrying about having an extra one in your bag. Physical insecurities such as [6]digital forensics on cell phones, even

[7]counter-offerings are today's reality, while [8]flexible lawful wiretapping may still be taking one way or another – I guess the NSA got all the attention recently, with their domestic spying program.

As the [9]Mindmaker pointed out, we must assume that we are trackable wherever we go, but I think this

dependence would get even more abused in the future by the time proposed laws match with the technology.

1. [http://photos1.blogger.com/blogger/1933/1779/1600/celltrack\\_485.9.jpg](http://photos1.blogger.com/blogger/1933/1779/1600/celltrack_485.9.jpg)
2. <http://ddanchev.blogspot.com/2006/03/privacy-issues-related-to-mobile-and.html>
3. [http://www.wired.com/news/politics/privacy/0,70829-0.html?tw=wn\\_technology\\_2](http://www.wired.com/news/politics/privacy/0,70829-0.html?tw=wn_technology_2)
4. [http://cbs4boston.com/consumer/local\\_story\\_103104037.html](http://cbs4boston.com/consumer/local_story_103104037.html)
5. [http://www.oreillynet.com/etel/blog/2006/04/diy\\_cell\\_phone\\_tracking\\_with\\_m.html](http://www.oreillynet.com/etel/blog/2006/04/diy_cell_phone_tracking_with_m.html)
6. <http://ddanchev.blogspot.com/2006/04/digital-forensics-efficient-data.html>
7. <http://www.sms007.cz/>
8. <http://www.nydailynews.com/front/v-pfriendly/story/399892p-338804c.html>
9. <http://www.blogcharm.com/Singularity>

306

### **Wiretapping VoIP Order Questioned (2006-05-09 20:17)**

[1]There's been a lot of buzz recently on the FCC's [2]order [3]requiring all VoIP providers to begin compliance with

[4]CALEA in order to lawfully intercept VoIP communications by the middle of 2007 . Yesterday, a U.S judge seems to

have [5]challenged the order, from the article :

*" The skepticism expressed so openly toward the administration's case encouraged civil liberties and education*

*groups that argued that the U.S. is improperly applying telephone-era rules to a new generation of Internet services.*

*"Your argument makes no sense," U.S. Circuit Judge Harry T. Edwards told the lawyer for the Federal Communications Commission, Jacob Lewis. "When you go back to the office, have a big chuckle. I'm not missing this. This is ridiculous.*

*Counsel!' The Justice Department, which has lobbied aggressively on the subject, warned in court papers that*

*failure to expand the wiretap requirements to the fast-growing Internet phone industry "could effectively provide a surveillance safe haven for criminals and terrorists who make use of new communications services. "*

What's worth mentioning is that on a wide scale VoIP services are often banned in many countries, ISPs don't

tend to tolerate the traffic which on the other hand directly bypasses their VoIP offers, and even [6]China, one of

the largest telecom market continues to have [7]concerns about VoIP. Companies also seem to be [8]revising their

practices while trying to block Skype, among the most popular VoIP applications. Rather interesting, T-Mobile just

[9]announced that it would ban VoIP on its 3G network, but is it inability to achieve compliance or direct contradiction



with their business practices?

Whatever the reason, [10]VoIP communications aren't everyone's favorite, but represent a revolution in cheap, yet reliable communications. The more easily a network is made wiretap-ready, the easier for attackers in both, the short, and the long-term to abuse the backdoored idea itself, so don't. You can actually go through the [11]2005's

Wiretap Report and figure out the cost of wiretapping, limiting it by promoting insecure networks isn't going to solve

anything, given you actually know what you're [12]looking for at the bottom line.

Image courtesy of EFF's [13]"Monsters of Privacy" Animation.

Related resources :

[14]VoIP, FCC, CALEA

[15]Communications Assistance for Law Enforcement Act and Broadband Access and Services

[16]Secure VoIP - Zfone

[17]Sniffing VoIP Using Cain

[18]Oreka VoIP Sniffer

1.

[http://photos1.blogger.com/blogger/1933/1779/1600/monster\\_calea.0.jpg](http://photos1.blogger.com/blogger/1933/1779/1600/monster_calea.0.jpg)

2. [http://hraunfoss.fcc.gov/edocs\\_public/attachmatch/DOC-265221A1.pdf](http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-265221A1.pdf)

3. <http://www.voip-news.com/news/calea-voip-050406/>

4. <http://www.eff.org/Privacy/Surveillance/CALEA/>

5. [http://www.technologyreview.com/read\\_article.aspx?id=16800](http://www.technologyreview.com/read_article.aspx?id=16800)

307

6. <http://news.ft.com/cms/s/875630d4-cef9-11da-925d-0000779e2340.html>

7. <http://www.computerworld.com.au/index.php/id;699360484;fp;4;fpid;15>

8. <http://www.computerworld.com.au/index.php/id;1778030134;fp;16;fpid;0>

9. <http://news.zdnet.co.uk/communications/3ggprs/0,39020339,39267682,00.htm>

10. <http://www.upi.com/SecurityTerrorism/view.php?StoryID=20060411-013136-5394r>

11. <http://www.uscourts.gov/wiretap05/contents.html>

12. <http://ddanchev.blogspot.com/2006/03/data-mining-terrorism-and-security.html>

13. <http://www.eff.org/Privacy/Monsters/>

14. <http://www.cybertelecom.org/voip/fcccalea.htm>

15. <http://cryptome.org/fcc101305.txt>
16. <http://www.philzimmermann.com/EN/zfone/index.html>
17. <http://www.irongeek.com/i.php?page=videos/cainvoip1>
18. <http://oreka.sourceforge.net/>

308

### **Snooping on Historical Click Streams (2006-05-11 12:16)**

In a previous post "[1]The Feds, Google, MSN's reaction, and how you got "bigbrothered"? I gave practical advices on how can easily do your homework on the popularity of certain search terms and sites, without the need of issuing a

subpoena. The other day, [2]AlltheWeb (Yahoo!) introduced their [3]Livesearch feature, seems nice, still it basically

clusters possible opportunities. Now the interesting part, on the next day Google [4]launched [5]Google Trends

which is :

*" builds on the idea behind the Google Zeitgeist, allowing you to sort through several years of Google search*

*queries from around the world to get a general idea of everything from user preferences on ice-cream flavors to the*

*relative popularity of politicians in their respective cities or countries. "*

This is what I've been waiting for quite some time, and you can easily make very good judgements on key top-

ics based on regions, languages, even cities – marketers get yourself down to business!

[6]Antivirus, [7]Malware, [8]Spyware, [9]NSA, [10]Censorship, [11]Privacy

What's next, the rise of [12]MyWare and its integration on the Web? Give a try to [13]Yahoo!'s Buzz, and

[14]PacketStormSecurity's instant StormWatch as well.

1. <http://ddanchev.blogspot.com/2006/01/feds-google-msns-reaction-and-how-you.html>
2. <http://www.alltheweb.com/>
3. <http://livesearch.alltheweb.com/?ek=1>
4. <http://googleblog.blogspot.com/2006/05/yes-we-are-still-all-about-search.html#links>
5. <http://www.google.com/trends>
6. <http://www.google.com/trends?q=antivirus>
7. <http://www.google.com/trends?q=malware&ctab=0&date=all&geo=all>
8. <http://www.google.com/trends?q=spyware>
9. <http://www.google.com/trends?q=nsa>
10. <http://www.google.com/trends?q=censorship>
11. <http://www.google.com/trends?q=privacy>
12. <http://yro.slashdot.org/article.pl?sid=06/01/19/173226&from=rss>

13. <http://buzz.yahoo.com/>

14. <http://www2.packetstormsecurity.org/cgi-bin/search/stormwatch.cgi>

309

### **Pass the Scissors (2006-05-11 12:46)**

[1][2]Counterfeiting U.S currency is a profitable business given its stability and actual valuation, and so is [3]money

printing! It's just that sometimes there are too much legally printed money as well, and the [4]Fed is raising the

interest rates for the sixteenth time during the last two years - which doesn't stop it from making a buck in between.

Did you know you could get [5]Uncut Currency sheets " of fresh crisp new \$1.00, \$2.00, \$5.00, \$10.00 and

*\$20.00 greenbacks right off the press will delight someone special in your life. They make an especially unique gift for that "hard-to-buy-for" person."*

While I always joke that availability stands for temptation, that's a "process utilization" worth envying, but too much money available [6]isn't always a good thing.

1. [http://photos1.blogger.com/blogger/1933/1779/1600/currency\\_sheets.1.jpg](http://photos1.blogger.com/blogger/1933/1779/1600/currency_sheets.1.jpg)

2. [http://en.wikipedia.org/wiki/Counterfeit\\_United\\_States\\_currency](http://en.wikipedia.org/wiki/Counterfeit_United_States_currency)

3. <http://www.moneyfactory.gov/>

4. <http://news.ft.com/cms/s/720afafe-e08b-11da-9e82-0000779e2340.html>
5. <http://www.moneyfactory.gov/store/section.cfm/69>
6. <http://en.wikipedia.org/wiki/Inflation>

310

### **Is Bin Laden Lacking a Point? (2006-05-11 13:27)**

[1]If I were to name the masters of PSYOPS, that would be terrorists, who without a super power's financial capabili-

ties still manage to achieve the "media echo" effect they seem to be so good at. As you will eventually read in case you haven't though about it before, to me Al Jazeera always seems to be the launching platform given its strategic

position in the region, and the rest of the world's media are the disseminators - anything fresh and terrorism related

increases ratings.

Yesterday, I came across to a [2]translated version of Bin Laden's most recent "State of Jihad" speech April 23, 2006, and I feel blaming the "infidels" for whatever goes around the world, or taking anything against Islam

personally, is a very weak point. From the article :

*" One more time Al Jazeera promotes an Usama Bin Laden speech. After airing portions of the Bin Laden audio-*

*tape al Jazeera posted large fragments of the "speech" on its web site. This was the longest version possible we were able to have access to. After careful reading, my*

*assessment of the "piece" got reinforced: This is not just another audiotope or videotape of a renegade in some cave.*

*Regardless of who is the speaker and his whereabouts, the 30 minutes long read statement is a declaration,*

*probably as important as the February 1998 declaration of war against America, the Crusaders and their allies.*

*Imagine yourself as an Arab viewer: The speech was repeated endlessly throughout the day. Bin Laden didn't have*

*his 20 minutes of shine, but 24 hours at least. The Bin Laden audiotope wasn't played one or two times but until*

*every word was sinking deep in the minds of the attentive viewers. However the most powerful part of the speech*

*wasn't restricted to its content: Al Jazeera lined up the best of its "experts on Islamist groups" to react instantly to the audiotope and throughout the day, and add "more details and substance. "*

At the bottom line, religion still remains the opium of the masses and an excuse for not taking care of your

own destiny but expecting "someone else" to.

1. <http://photos1.blogger.com/blogger/1933/1779/1600/bin-laden-on-the-run.jpg>

2. [http://counterterrorismblog.org/2006/04/bin\\_ladens\\_state\\_of\\_jihad\\_spee.php](http://counterterrorismblog.org/2006/04/bin_ladens_state_of_jihad_spee.php)

## **Pocket Anonymity (2006-05-11 14:07)**

While the threats posed by improper use of removable media will continue to make headlines, here's a company that's offering the complete [1]all-in-one pocket anonymity solution - at least that's how they position it. From the [2]article :

*" Last month, a company called Stealth Ideas Inc. of Woodland Hills, Calif., came out with its StealthSurfer II ID*

*Protect. The miniature flash drive lets you surf anonymously from any computer using an integrated browser that*

*runs in an encrypted mode. It comes loaded with several tools, including Anonymizer Anonymous Surfing 1.540*

*(which has IP masking), RoboForm Pass2Go 6.5.9 (a user ID/password management application) and Thunderbird*

*1.0.7 (for e-mail access). But before you buy, check to see if the company has upgraded its browser, which, according to company officials at the product's launch, is Firefox 1.5.0.1. US-CERT and others have warned about significant*

*vulnerabilities in certain versions of Firefox (and Thunderbird, for that matter). The version available as of press time, Version 1.5.0.2, addresses those flaws. "*

Is the Anonymizer behind the idea, or is it a middleman trying to add value to the Anonymizer's existing offer,

and harness the brand powers of Firefox and Hushmail all in one? Wise, but the entire idea of [3]anonymity is based



on the Anonymizer's service, when anonymity still can be freely achieved to a certain extent. Very portable idea, the

thing is there are already free alternatives when it comes to pocket anonymity and that's [4]TorPark: Anonymous

browsing on a USB drive, and I think I can live without the enhancements.

1. <http://www.stealthsurfer.biz/>
2. [http://www.gcn.com/print/25\\_11/40668-1.html](http://www.gcn.com/print/25_11/40668-1.html)
3. <http://ddanchev.blogspot.com/2006/01/anonymity-or-privacy-on-internet.html>
4. <http://torpark.nfshost.com/>

312

### **Travel Without Moving - Scratching the Floor (2006-05-11 14:55)**

You don't really need a [1]reconnaissance satellite to spot this, it's precisely the type of "sight" you can see for yourself on daily basis – but he's still moving isn't he? :)

1. <http://ddanchev.blogspot.com/2006/05/travel-without-moving-typhoon-class.html>

313

### **Terrorist Social Network Analysis (2006-05-12 20:09)**

[1]In previous posts "[2]Visualization, Intelligence and the Starlight project" and "[3]Visualization in the Security and New Media world" I covered various security and intelligence related projects and mostly emphasized on the future

potential of visualizing data. [4]Data mining is still [5]everyday's reality – social networking as well. Just came across this at [6]DefenseTech :

*" It'd be one thing if the NSA's massive sweep of our phone records was actually helping catch terrorists. But*

*what if it's not working at all? A leading practitioner of the kind of analysis the NSA is supposedly performing in this surveillance program says that "it's a waste of time, a waste of resources. And it lets the real terrorists run free."*

*Re-reading the USA Today [7] piece, one paragraph jumped out: This kind of data collection from phone companies is not uncommon; it's been done before, though never on this large a scale, the official said. The data are used*

*for 'social network analysis,' the official said, meaning to study how terrorist networks contact each other and how they are tied together. So I called [8] Valdis Krebs, who's considered by many to be the leading authority on [9] social network analysis– the art and science of finding the important connections in a seemingly-impenetrable mass of data.*

*His [10] analysis of the social network surrounding the 9/11 hijackers is a classic in the field. "*

It gets even more interesting with a [11]comparison of a Fortune 500 company's network and Al Qaeda's one.

Social networks are among the driving forces of Web 2.0, and I find the concept of communication and planning

online a [12]very realistic one. And if you really want to know more about social networks in the business world,

corporate anthropologist [13]Karen Stephenson - The Organization woman is really up to it, very good article. And of

course, [14]Valdis Krebs's blog on smart economic networks.

1. [http://photos1.blogger.com/blogger/1933/1779/1600/step\\_2.gif](http://photos1.blogger.com/blogger/1933/1779/1600/step_2.gif)
2. <http://ddanchev.blogspot.com/2006/01/visualization-intelligence-and.html>
3. <http://ddanchev.blogspot.com/2006/03/visualization-in-security-and-new.html>
4. <http://ddanchev.blogspot.com/2006/03/data-mining-terrorism-and-security.html>
5. [http://www.usatoday.com/news/washington/2006-05-10-nsa\\_x.htm](http://www.usatoday.com/news/washington/2006-05-10-nsa_x.htm)
6. <http://www.defensetech.org/archives/002399.html>
7. [http://www.usatoday.com/news/washington/2006-05-10-nsa\\_x.htm](http://www.usatoday.com/news/washington/2006-05-10-nsa_x.htm)
8. <http://www.orgnet.com/VKbio.html>
9. <http://www.tcf.org/list.asp?type=NC&pubid=1239>
10. <http://www.orgnet.com/prevent.html>
11. <http://www.defensetech.org/archives/002402.html>
12. <http://ddanchev.blogspot.com/2006/01/cyberterrorism-recent-developments.html>

13.

[http://money.cnn.com/magazines/business2/business2\\_archive/2006/04/01/8372807/index.htm](http://money.cnn.com/magazines/business2/business2_archive/2006/04/01/8372807/index.htm)

14. <http://www.networkweaving.com/blog/>

314

## **Valuing Security and Prioritizing Your Expenditures (2006-05-15 14:16)**

[1]I often blog on various market trends related to information security and try to provide an in-depth coverage of

emerging or current trends - in between active comments. In previous posts "[2]FBI's 2005 Computer Crime Survey

- what's to consider?", "[3]Spotting valuable investments in the information security market", "[4]Why we cannot measure the real cost of cybercrime?", "[5]Personal Data Security Breaches - 2000/2005" and, "[6]To report, or not to report?" I emphasized on the following key points in respect to data security breaches and security investments :

- on the majority of occasions companies are taking an outdated approach towards security, that is still living

in the perimeter based security solutions world

- companies and data brokers/aggregators are often reluctant to report security breaches even

when they have the legal obligation to due to the fact that, either the breach still hasn't been detected, or the lack

of awareness on what is a breach worth reporting

- the flawed approaches towards quantifying the costs related to Cybercrime are resulting in overhyped state-

ments in direct contradiction with security spending

- companies still believe in the myth that spending more on security, means better security, but that's not al-

ways the case

- given the flood of marketing and the never ending "media echo" effect, decision makers often find them-

selves living with current trends, not with the emerging ones, which is what they should pay attention to

It is often mistaken that the more you spend on security, the higher level of security would be achieved, whereas

that's not always the case - it's about prioritizing and finding the most suitable metrics model for your investment.

Here's an [7] article describing exactly the same impression :

*" Security breaches from computer viruses, spyware, hacker attacks and equipment theft are costing British*

*business billions of pounds a year, according to a survey released Tuesday. The estimated loss of \$18 billion (10*

*billion pounds) is 50 percent higher than the level calculated two years ago, according to the survey that consultancy PricewaterhouseCoopers conducted for the U.K. Department of Trade and Industry. The rise comes despite the fact*

*that companies are increasing their spending on information security controls to an average 4 percent or 5 percent*

*of their IT budget, compared with 3 percent in 2004. "*

315

That's pretty much the situation everywhere, companies are striving to apply metrics to security investments and this is where it all gets blur. Spending more on security might seems to be logical answer, but start from the

fact that open networks, thus exposed to a great deal of uncontrollable external factors, undermine the majority of

models so far. Bargaining with security, or "[8]Getting paid for getting hacked" remains a daily practice whatsoever.

Let's consider various social aspects concerning the participants.

**A financial executive often wants to know more on :**

- Do I get any return on my investment (ROI) ?
- What % of the risk is mitigated and what are your benchmarking methods?
- What may I lose if I don't invest, and where's the sweet spot?
- How much is enough?
- How do I use basic financial concepts such as diversification in the security world?
- How would productivity be influenced due to the lack of solutions, or even their actual use?

A security consultant on the other hand might be interested in – How do I convince senior management in

the benefits of having a honeyfarm in respect to mitigating the overall risk of having real systems breached into,

without using Cyberterrorism as the basis of discussion?

These different school's of thought, positions, responsibilities and budget-allocation hungry individuals are con-

stantly having trouble communicating with each other. And while you cannot, and perhaps even should not try to

educate your security workforce in to the basics of finance, an understanding of both side's point of view may change

things - what you don't see value in, is often someone else's treasure.

Another [9]recent article on the topic of justifying security expenditure, or mostly assigning value made me

an impression :

*" So we came up with Value Protection," Larson says.*

*"You spend time and capital on security so that you*

*don't allow the erosion of existing growth or prevent new growth from taking root. The number-one challenge for*

*us is not the ability to deploy the next, greatest technology. That's there. What we need to do now is quantify the*

*value to the business of deploying those technologies." "It adds value; we're very supportive of it," says Steve Schmitt, American Water's vice president of operations, of Larson's Value Protection metric. For a while, people were just*

*trying to create reasonable security, Schmitt says, "but now you need something more—something that proves the*

*value, and that's what Bruce developed. Plus, as a secondary benefit, it's getting us better visibility from business owners and partners on risks and better ways to mitigate the risks. "*

Good point on first estimating the usefulness of current technologies, before applying the "latest", or "newest" ones.

The rest comes to the good old flaws in the ROSI model, how would you be sure that it would be the \$75,000 virus

316

outbreak that will hit your organization, and not the \$5000 one? "[10]Return On Security Investment (ROSI) - A Practical Quantitative Model" emphasized on the challenges to blindly assigning the wrong value to a variable :

*" The virus scanner appears to be worth the investment, but only because we're assuming that the cost of a*

*disaster is \$25,000, that the scanner will catch 75 % of the viruses and that the cost of the scanner is truly \$25,000. In reality, none of these numbers are likely to be very accurate. What if three of the four viruses cost \$5,000 in damages but one costs \$85,000? The average cost is still \$25,000. Which one of those four viruses is going to get past the*

*scanner? If it's a \$5,000 one, the ROSI increases to nearly 300 % - but if it's the expensive one, the ROSI becomes*

*negative! "*



Among the first things to keep in mind while developing a risk management plan, is to identify the assets,

identify the potential attackers, and find ways to measure the threat exposure and current threatscape as well. In a

publication I wrote three years ago, "[11]Building and Implementing a Successful Information Security Policy", that as a matter of fact I still find a quality and in-depth reading on the topic, I outlined some ideas on achieving the full effect of the abovementioned practices – it's also nice to come across it given in [12]assignments and discussed in

[13]lectures too. An excerpt on Risk Analysis :

"

*As in any other sensitive procedure, Risk Analysis and Risk Management play an essential role in the proper func-*

*tionality of the process. Risk Analysis is the process of identifying the critical information assets of the company and their use and functionality – an important (key) process that needs to be taken very seriously. Essentially, it is the very process of defining exactly WHAT you are trying to protect, from WHOM you are trying to protect it and most*

*importantly, HOW you are going to protect it. "*

Identifying the threats and some current threats worth keeping in mind

- windows of opportunities/0day attacks
- lousy assets/vulnerability/patch management
- insecure end users' habits

- sneaky and sophisticated malicious software
- wireless/bluetooth information leakage
- removable media information leakage

### **How would you go for measuring the risk exposure and risk mitigated factor?**

Risk exposure and risk mitigated are both interesting and hard to quantify, should we consider the whole pop-

ulation given we somehow manage to obtain fresh information on the current threats ( through the use of Early

Warning System such as [14]Symantec's DeepSight Analyzer, [15]The Internet Storm Center, or [16]iDefense's

Intelligence services for instance). Today, it is often based on :

317

- the number of workstations and network assets divided by the historical occurrence of a particular security event on the network - the use of mobile agents for the specifics of a company's infrastructure effects is hard

sometimes

- on the historical TCO data related to typical breaches/security events

Risk mitigated is often tackled by the use of Best practices - whether outdated or relevant is something else,

Cyber Insurance and the current, sort of, scientifically justified ROSI model are everyday's practice, but knowing

the inner workings of your organization and today's constantly changing threatscape and how it(if) affects you is a key practice while prioritizing expenditure. You cannot, and should not deal with all the insecurities facing your organization, instead consider prioritizing your security expenditure, not just following the daily headlines and vendor-released, short-term centered research.

It's hard to quantify intellectual property's value, the way it's hard to quantify TCO losses due to security breaches

and it's perhaps the perfect moment to mention the initiative that I undertook in the beginning of this year - a 50/50

security/financial cross-functional team on coming up with a disruptive idea - more on the current status soon, still,

thanks for the time and efforts folks! To sum up, a nice quote by the authors of the research I mentioned : "*Most of the problems stem from the fact that security doesn't directly create anything tangible - rather it prevents loss. A loss that's prevented is a loss that you probably won't know about.*"

At the bottom line, are you making money out of having security, that is thinking business continuity, not con-

tingency planning, and should we keep on trying to adapt financial concepts, and not rethinking them all?

Recommended reading/resources on the topic of justifying security expenditure :

- [17]Return on Information Security Investment
- [18]Risk - A Financial Overview
- [19]Calculated Risk - Guide to determining security ROI
- [20]The Return on Investment for Network Security
- [21]Analysis of Return on Investment for Information Security
- [22]Methodologies for Evaluating Information Security Investments
- [23]Risk Assessment for Security Economics - very informative slides
- [24]Economics and Security Resource page
- [25]Information Security in the Extended Enterprise: Some Initial Results From a Field Study of an Industrial Firm
- [26]PKI and Financial Return on Investment
- [27]Privacy Breach Impact Calculator
- [28]Guide to Selecting Information Technology Security Products

1.

<http://photos1.blogger.com/blogger/1933/1779/1600/value.jpg>

2. <http://ddanchev.blogspot.com/2006/01/fbis-2005-computer-crime-survey-whats.html>

3. <http://ddanchev.blogspot.com/2006/04/spotting-valuable-investments-in.html>

4. <http://ddanchev.blogspot.com/2006/01/why-we-cannot-measure-real-cost-of.html>
5. <http://ddanchev.blogspot.com/2006/01/personal-data-security-breaches.html>
6. <http://ddanchev.blogspot.com/2006/01/to-report-or-not-to-report.html>
7. <http://news.zdnet.co.uk/internet/security/0,39020375,39265531,00.htm>
8. [http://ddanchev.blogspot.com/2006/03/getting-paid-for-getting-hacked\\_17.html](http://ddanchev.blogspot.com/2006/03/getting-paid-for-getting-hacked_17.html)
9. [http://www.csoonline.com/read/040106/value\\_visible.html](http://www.csoonline.com/read/040106/value_visible.html)
10. [http://www.securemark.us/downloads/ROSI-Practical\\_Model-20050406.pdf](http://www.securemark.us/downloads/ROSI-Practical_Model-20050406.pdf)
11. <http://www.windowsecurity.com/pages/security-policy.pdf>
12. [http://dcm.cl.uh.edu/nsfsecurity/public/Modules/AYang\\_Module/admi1/Assignment1/Admi1Assign1.html](http://dcm.cl.uh.edu/nsfsecurity/public/Modules/AYang_Module/admi1/Assignment1/Admi1Assign1.html)
13. <http://ece.gmu.edu/~gmartin/fall05/tcom562-f05.htm>
14. <http://analyzer.symantec.com/>
15. <http://isc.sans.org/>
16. <http://www.idefense.com/>

17. [http://www.infosecwriters.com/text\\_resources/pdf/ROIsl.pdf](http://www.infosecwriters.com/text_resources/pdf/ROIsl.pdf)
18. <http://www.csoononline.com/read/110104/interview.html>
19. <http://www.csoononline.com/read/120902/calculate.html>
20. [http://www.cisco.com/warp/public/cc/so/neso/sqso/roi4\\_wp.pdf](http://www.cisco.com/warp/public/cc/so/neso/sqso/roi4_wp.pdf)
21. <http://www.getronics.com/NR/rdonlyres/en6bl7yole4i5vzvzzrl5ud3klueu2ex5mnyt2it3zwuivhfkenfftpxjn3gsewh3bihoeconfdy3u5x33zpw2mq1b/SecurityROI.pdf>
22. <http://csrc.lse.ac.uk/asp/aspecis/20050136.pdf>
23. <http://www.dmi.unict.it/~giamp/wsf/05Material/spagnulo.pdf>
24. <http://www.cl.cam.ac.uk/~rja14/econsec.html>
25. <http://infosecon.net/workshop/pdf/51.pdf>
26. [http://www.pkiforum.org/pdfs/Financial\\_Return\\_on\\_Investment.pdf](http://www.pkiforum.org/pdfs/Financial_Return_on_Investment.pdf)
27. [http://searchsecurity.techtarget.com/general/0,295582,sid14\\_gci1182844,00.html?track=NL-430&ad=551180](http://searchsecurity.techtarget.com/general/0,295582,sid14_gci1182844,00.html?track=NL-430&ad=551180)
28. <http://csrc.nist.gov/publications/nistpubs/800-36/NIST-SP800-36.pdf>

## **EMP Attacks - Electronic Domination in Reverse (2006-05-16 14:21)**

[1]Yesterday, I came across to an updated(April 14, 2006)  
CRS report - [2]High Altitude Electromagnetic Pulse (HEMP)

and High Power Microwave (HPM) Devices: Threat  
Assessments, a topic I covered in a previous post related to

[3]asymmetric warfare.

Basically, it outlines critical issues such as, what is the  
U.S(or pretty much any other country thinking asymmetric  
warfare) doing to ensure critical civil infrastructure is  
protected against EMP attacks, how does the vulnerability of  
EMP attacks encourage other nations to develop such  
capabilities, and yes, of course the "threat" of terrorist EMP  
warfare – in your wildest dreams only. An excerpt :

*" However, other analysts maintain that some testing done  
by the U.S. military may have been flawed, or in-*

*complete, leading to faulty conclusions about the level of  
resistance of commercial equipment to the effects of EMP.*

*These analysts point out that EMP technology has been  
explored by several other nations, and as circuitry becomes*

*more miniaturized, modern electronics become increasingly  
vulnerable to disruption. They argue that it could possibly  
take years for the United States to recover fully from  
widespread damage to electronics resulting from a large-  
scale EMP attack. "*

Why wouldn't a "reported sponsor of terrorist" nations wage EMP warfare, or even try to over the U.S? Be-

cause they would have the U.S in their backyard in less than a day, but the opportunity to balance the powers, or

achieve temporary military advantage given the attack remains undetected is a tempting factor for future develop-

ments - the ongoing miniaturization and the fact that intense energy effects can be can be produced without an

A-Bomb makes it even worse. Surgical HPM and EMP attacks without fear of retaliation is what possible adversaries

could be aiming at, and of course portability :

*" Other HPM weapons being tested by the military are portable and re-usable through battery-power, and are*

*effective when fired miles away from a target. These weapons can also be focused like a laser beam and tuned to*

*an appropriate frequency in order to penetrate electronics that are heavily shielded against a nuclear attack. The*

*deepest bunkers with the thickest concrete walls reportedly are not safe from such a beam if they have even a single unprotected wire reaching the surface. "*

Yesterday I was looking for an article I wrote in 1998 on Nuclear Weapons and seem to have found it - it

makes me smile given my age, and the fact that I had to orally defend the topic, hope you will find it an interesting

retro read :) I don't necessarily agree with all the things, it just the way I was perceiving the world back then. For



instance, Russia didn't accelerate their scientific efforts, as the A-bomb secret eventually leaked out to them, and

with the fall of the Soviet Union and ICBMs available in every corner of the country and its republics, it wasn't hard for other nations to piggyback too.

320

Did you know that Stalin was aware of the U.S's A-bomb, [4]even [5]before Harry Truman was? – the consequence of too much secrecy sometimes!

## **Nuclear Weapons**

There has always been war, and will always be though we live in more peaceful world nowadays. It's a long time that

nuclear weapons are not the same threat to the world's peace as they were years ago. Despite all the reduction

and limitation of nuclear weapons they haven't disappeared yet completely. Today all the nuclear arsenals are able

to kill everybody on EARTH, a thousand times, though nobody wants to die even once. One of the greatest scientific

and human's achievements - mastering the nuclear energy, is in position both to change the traditional sources of

energy, and to move toward the social progress. However, this discovery was used not in people's behalf, but against

it.

During Truman's leadership nuclear scientists were working on the project "MANHATTAN" as they were to fin-

ish mastering the nuclear energy, but they didn't know that their discovery would change completely the world to

worse, demanding death to million people. Americans have always been competing with Russians in each sphere.

When Americans discovered the A-BOMB Russians were far from it. Then Truman decided to drive Russia into a

corner. But he didn't have the chance, due to Stalin who ostensibly didn't pay attention to the threat. To show his

power Truman threw the A-BOMB on Hiroshima on 6 of August at 8 :00 am. It generated a huge amount of energy

when it exploded. Most people died within a few hours. By the end of 1945 the estimated number of people who died

as a direct result of the bomb was 140,000. But later it has been concluded that the number of people who died was

approximately 200,000, even more. Russia decided that it couldn't last so long and accelerated the speed of doing

their project for the A-BOMB several times. Only for 4 years they worked it out which the Americans succeeded for

20. As Russia's A-BOMB appeared the United State's plans for starting a war and attack Russia made them think.

All their plans went wrong. When the U.S controlled the weapons of mass destruction their strategists used

to think about the harmful power of the weapons. Now, the U.S have completely changed their policy line. When

a conflict arise anywhere in world they would help. When a disaster damages a country, when a war starts they

always stand by the side of the weaker. They mastered outer space and they don't do it just for themselves but for

the whole mankind. Now all the people in world develop good relationships. But we live in a troubled world. Our

daily cares are increasingly dwarfed by the thought that they may vanish in a flash. People separated by continents

and oceans are united in their wish to prevent the global nuclear catastrophe. Young people today do not wish war

they want peace and love. It's not just a wish, it's a must!

This is eight years ago, and I'm still keeping the spirit I guess :)

1.

<http://photos1.blogger.com/blogger/1933/1779/1600/EMP.jpg>

2. <http://www.fas.org/sgp/crs/natsec/RL32544.pdf>

3. <http://ddanchev.blogspot.com/2006/02/who-needs-nuclear-weapons-anymore.html>

4. <http://www.dannen.com/decision/potsdam.html>

5. <http://killeenroos.com/5/bomb/decision.htm>

321

**Insider Competition in the Defense Industry (2006-05-16 14:49)**

[1]While there aren't any [2]smoking emails mentioned in this case, where else can we spot [3]insiders if [4]not in

the defense industry, an industry where securing government-backed contracts, or teasing military decision makers

with the latest technologies ensures the long-term existence of the business itself? From the [5]article :

*" Boeing has been under investigation for improperly acquiring thousands of pages of rival Lockheed Martin's*

*proprietary documents in the late 1990s, using some of them to help win a competition for government rocket-*

*launching business. The government stripped Boeing of about \$1 billion worth of rocket launches for its improper use of the Lockheed documents. "*

[6]Boeing and [7]Lockheed Martin remain the key players in the defense industry, ensuring their portfolio of

services (cyberwarfare, theater warfare, grid networking compatibility etc.) remain competitive. I once said that

during the Cold War, the tensions between the U.S and the Soviet Union used to be the driving force of progress and

innovation, these days, terrorism is the driving force and the "excuse" for military and intelligence spending. And while NASA's budget has been decreasing with the time, the next major space innovation wouldn't come from NASA,

but from the commercial sector.

What's the bottom line?

A minor short-term effect, and long-term business continuity for sure as " *Boeing*

*shares fell \$1.76, or 2 percent, to \$85.25 in morning trading on the New York Stock Exchange. "*

1. <http://photos1.blogger.com/blogger/1933/1779/1600/insider-trading.1.gif>
2. <http://ddanchev.blogspot.com/2006/02/smoking-emails.html>
3. <http://ddanchev.blogspot.com/2005/12/insiders-insights-trends-and-possible.html>
4. <http://ddanchev.blogspot.com/2006/04/insider-fined-870.html>
5. [http://www.businessweek.com/ap/financialnews/D8HKAJMO2.htm?campaign\\_id=apn\\_home\\_down&chan=db](http://www.businessweek.com/ap/financialnews/D8HKAJMO2.htm?campaign_id=apn_home_down&chan=db)
6. [http://www.boeing.com/product\\_list.html](http://www.boeing.com/product_list.html)
7. <http://www.lockheedmartin.com/wms/findPage.do?dsp=fec&ci=5&sc=400>

322

## **Techno Imperialism and the Effect of Cyberterrorism (2006-05-16 15:20)**

It's been a while since I've last blogged [1]about [2]Cyberterrorism, and while many did mentioned the topic in

between the recent [3]DRDoS attacks, Cyberterrorism is so much more than simply shutting down the Internet,

namely the ability to communicate, research, recruit and use propaganda to achieve goals based on ideological

beliefs, or the convergence of Terrorism and the Internet.

Can we argue that cyberterrorism is the direct effect of [4]techno imperialism, or let's use a more friendly

word such as IT-dependent society and information infrastructure?

What exactly does cyberterrorism mean? When does an average internet user's malicious activity turns into

cyberterrorism ones? Are there clear definitions, or the lack of such as resulting in the in a total misunderstanding for both, the media and the general public. The recently released Google Trends, which I covered in a previous [5]post,

doesn't even count Cyberterrorism, so I looked further and came across to a very good research "[6]Fear-mongering

or fact: The construction of 'cyber-terrorism' in U.S., U.K, and Canadian news media" that aims to emphasize on the common misunderstanding when defining Cyberterrorism and the media's acceptance of the concept. The outcome?

Declining media presence with the years, to end up where it is [7]today, but what you should keep in mind is that

the concept is still out there.

Trying to separate Cyberterrorism as a tool for achieving Information Warfare dominance is like on purposely

ignoring the the big picture – that Cyberterrorism, one that sometimes results out of [8]hacktivism tensions is a pow-

erful tool for achieving the full effect of information warfare. Whereas such attacks occur all the time, I can argue that the actual impact of cyberterrorism cannot be easily and quantitatively justified. We all know that it's theoretically

logical for terrorists to use the Internet for various cyberplanning and cyber communication, what can we do about it?

[9]Crawling for terrorist web sites clearly associated with different organizations, or trying to spot terrorist

sympathizers have been in the execution stage for yers. Projects such as the [10]Terrorism Knowledge Discovery

Project, take a very deep look into the subject by introducing Terrorism Knowledge Portal, an aggregated source for

intelligence. Moreover, according to a recent [11]article :

*" SAIC has a \$US7 million Defence Department contract to monitor 1500 militant websites that provide al Qaeda and other militant organisations with a main venue for communications, fund-raising, recruitment and training. "*

It's also interesting to note other initiatives that started back in 2001, such as the [12]Automatic Identification of Extremist

Internet Web Sites.

Another concept goes in-depth into [13]Confronting Cyberterrorism with Cyber Deception as " *if it is possible*

*to deceive terrorists, then it should also be possible to deceive cyberterrorists. The reliance of cyberterrorists on*  
323

*information technology makes them vulnerable to cyber deceptions. In addition, many of the methods and tools that cyberterrorists would use are similar to those used by other less malicious hackers, so we can plan specific deceptions to use against them in advance. "* As you can see on the grid above, the actors, the deception target and the level of difficulty provide more insight into the idea, great research!

Steganography embedded images used by terrorists on the public web can be doubtful, but on the Dark Web,

why not? According to a [14]research I came across to some time ago :

" *In academia, graduate students Niel Provos and Richard Honeyman at the University of Michigan have writ-*

*ten a web crawling program to detect steganographic images in the wild. The program has already digested 2 billion*

*JPEG's on popular sights such as ebay and has so far found only one stego-image in the wild. The detected image was*

*on an ABC web page that dealt with the topic of steganography. "*

[15]Detecting Steganographic Content on the Internet as a [16]concept has been around for ages, while plain



old encryption is the de-facto practice according to a well [17]researched news article :

- Wadih El Hage, one of the suspects in the 1998 bombing of two U.S. embassies in East Africa, sent encrypted

e-mails under various names, including "Norman" and "Abdus Sabbur," to "associates in al Qaida," according to the Oct. 25, 1998, U.S. indictment against him. Hage went on trial Monday in federal court in New York.

- Khalil Deek, an alleged terrorist arrested in Pakistan in 1999, used encrypted computer files to plot bomb-

ings in Jordan at the turn of the millennium, U.S. officials say. Authorities found Deek's computer at his Peshawar,

Pakistan, home and flew it to the National Security Agency in Fort Meade, Md. Mathematicians, using supercomput-

ers, decoded the files, enabling the FBI to foil the plot.

- Ramzi Yousef, the convicted mastermind of the World Trade Center bombing in 1993, used encrypted files

to hide details of a plot to destroy 11 U.S. airliners. Philippines officials found the computer in Yousef's Manila

apartment in 1995. U.S. officials broke the encryption and foiled the plot. Two of the files, FBI officials say, took

more than a year to decrypt.

324

Among the many cases I am aware of worth mentioning are :

- [18]What are the real risks of cyberterrorism? In 1998, a 12-year-old hacker broke into the computer system

that controlled the floodgates of the Theodore Roosevelt Dam in Arizona, according to a June Washington Post

report. If the gates had been opened, the article added, walls of water could have flooded the cities of Tempe and

Mesa, whose populations total nearly 1 million.

- [19]Cyberterrorism: How Real Is the Threat? Yonah Alexander, a terrorism researcher at the Potomac Institute—a

think tank with close links to the Pentagon—announced in December 2001, the existence of an “Iraq Net.” This

network supposedly consisted of more than one hundred websites set up across the world by Iraq since the

mid-1990s to launch denial-of-service or DoS attacks against U.S. companies. The concept of [20]botnets wasn’t that

popular at the time, so that’s an example of marginal thinking on acquiring DoS power.

- [21]In the indictment against Zacharias Moussaoui, it states that Moussaoui had among his possessions a

flight simulator program, software for reviewing pilot procedures for a Boeing 747 Model 400, and a computer disk

of information on aerial spraying of pesticides. The indictment also outlines Moussaoui’s use of e-mail to inquire about flight training.

- [22]For almost two years, intelligence services around the world tried to uncover the identity of an Internet

hacker who had become a key conduit for al-Qaeda. The savvy, English-speaking, presumably young webmaster

taunted his pursuers, calling himself Irhabi – Terrorist – 007. He hacked into American university computers,

propagandized for the Iraq insurgents led by Abu Musab al-Zarqawi and taught other online jihadists how to wield

their computers for the cause.

I can argue which article is more intriguing compared to [23]BusinessWeek's writeup on catching the [24]Shad-

owCrew, but anyway all you need to get a reader's attention is a name such as Abu Musab al-Zarqawi, a point that

I feel is totally brainwashed in this paragraph :)

325

Cyberterrorism is an inseparable part of Information Warfare, and while we would hopefully never witness a catastrophic scenario, that is offensive use of Cyberterrorism, recruitment and propaganda flood the Internet on a

daily basis. Just stop being suspicious about everyone, and try to enjoy life in between, can you, as terrorists are not everywhere – but where we see them at the bottom line!

1. <http://ddanchev.blogspot.com/2006/01/cyberterrorism-recent-developments.html>

2. <http://ddanchev.blogspot.com/2005/12/cyberterrorism-dont-stereotype-and-its.html>
3. [http://ddanchev.blogspot.com/2006/04/on-insecurities-of-internet\\_13.html](http://ddanchev.blogspot.com/2006/04/on-insecurities-of-internet_13.html)
4. <http://www.zmag.org/Sustainers/Content/2001-10/04healy.cfm>
5. <http://ddanchev.blogspot.com/2006/05/snooping-on-historical-click-streams.html>
6. [http://www.oii.ox.ac.uk/research/cybersafety/extensions/pdfs/papers/susan\\_keith.pdf](http://www.oii.ox.ac.uk/research/cybersafety/extensions/pdfs/papers/susan_keith.pdf)
7. <http://news.google.com/news?hl=en&ned=us&q=cyberterrorism&ie=UTF-8&scoring=d>
8. <http://ddanchev.blogspot.com/2006/02/hacktivism-tensions.html>
9. <http://ddanchev.blogspot.com/2006/02/look-whos-gonna-cash-for-evaluating.html>
10. [http://ai.arizona.edu/people/edna/AILab\\_terrorism%20Knowledge%20Discovery%20ISI%20\\_apr04.pdf](http://ai.arizona.edu/people/edna/AILab_terrorism%20Knowledge%20Discovery%20ISI%20_apr04.pdf)
11. [http://news.yahoo.com/s/nm/20060504/us\\_nm/security\\_videogames\\_dc\\_4](http://news.yahoo.com/s/nm/20060504/us_nm/security_videogames_dc_4)
12. <http://www.epic.org/privacy/choicepoint/acxiominternet.pdf>

13. [http://www.cs.nps.navy.mil/people/faculty/rowe/oldstudents/gtan\\_thesis\\_final.pdf](http://www.cs.nps.navy.mil/people/faculty/rowe/oldstudents/gtan_thesis_final.pdf)
14. <http://www.vu.union.edu/~queirolf/ESSAYS/Steganography.pdf>
15. <http://www.citi.umich.edu/techreports/reports/citi-tr-01-11.pdf>
16. <http://www.chromesplash.com/jcallinan.com/publications/steg.pdf>
17. <http://www.usatoday.com/tech/news/2001-02-05-binladen.htm>
18. [http://news.zdnet.com/2100-1009\\_22-955293.html](http://news.zdnet.com/2100-1009_22-955293.html)
19. <http://www.usip.org/pubs/specialreports/sr119.html>
20. <http://ddanchev.blogspot.com/2006/02/war-against-botnets-and-ddos-attacks.html>
21. [http://www.ists.dartmouth.edu/TAG/ITB/ITB\\_032004.pdf](http://www.ists.dartmouth.edu/TAG/ITB/ITB_032004.pdf)
22. [http://www.washingtonpost.com/wp-dyn/content/article/2006/03/25/AR2006032500020\\_pf.html](http://www.washingtonpost.com/wp-dyn/content/article/2006/03/25/AR2006032500020_pf.html)
23. [http://www.businessweek.com/magazine/content/05\\_22/b3935001\\_mz001.htm](http://www.businessweek.com/magazine/content/05_22/b3935001_mz001.htm)
24. [http://news.com.com/Photo+Shadowcrew+site+in+federal+custody/2009-7348\\_3-5431431.html](http://news.com.com/Photo+Shadowcrew+site+in+federal+custody/2009-7348_3-5431431.html)

## **Travel Without Moving - Cheyenne Mountain Operations Center (2006-05-22 17:16)**

[1]It's a small world – and a busy one, this post was supposed to appear the previous week so here it goes. There

are certain [2]places you just can't miss on the world's map, and the [3]Cheyenne Mountain Operations Center

is one of them. Remember the typical massive gate in the [4]War Games movie, or in pretty much any other

military/intelligence thriller you've watched? Try this one. [5]Nuke it, [6]EMP it, it's supposed to stand tall, yet it

remains a visible sensitive location for you to enjoy [7]without moving. The other day I came across to a report that I

somehow missed in relation to various threats – if any – posed by [8]Google Earth. "[9]Google Earth Study: Impacts and Uses for Defence and Security" is worth the [10]read :

*" The Google Earth study on the impacts and uses for defence and security is aimed at answering a number of questions. What are the technical features, the reliability and limits of GE data and software, regarding international security regulations? Which confidence in data, real dangers of a pernicious use, or impacts of such an easy access*

*to imagery is there on users or the geographical information market? What are the new applications stemming from*

*GE, which services can be derived from this application, or what are the ways to integrate GE into an information system? "*

Stay tuned for the upcoming Oday sights from around the world.

1.

[http://photos1.blogger.com/blogger/1933/1779/1600/dod\\_operations.jpg](http://photos1.blogger.com/blogger/1933/1779/1600/dod_operations.jpg)

2.

<http://maps.google.com/maps?f=q&hl=en&q=Cheyenne+Mountain&ll=38.744359,-104.84671&spn=0.00415,0.010729&t=k&om=1>

3. <https://www.cheyennemountain.af.mil/>

4. <http://ddanchev.blogspot.com/2006/03/dvd-of-weekend-war-games.html>

5. <http://ddanchev.blogspot.com/2006/02/who-needs-nuclear-weapons-anymore.html>

6. <http://ddanchev.blogspot.com/2006/05/emp-attacks-electronic-domination-in.html>

7. <http://ddanchev.blogspot.com/2006/05/travel-without-moving-scratching-floor.html>

8. <http://ddanchev.blogspot.com/2006/04/threat-by-google-earth-has-just.html>

9.

<http://www.fleximage.fr/generated/objects/Image/GEO%20Informatics%20v.2.pdf>

10.

<http://www.fleximage.fr/generated/objects/Image/GIS%20monitor.pdf>

327

### **Nation Wide Google Hacking Initiative (2006-05-23 18:21)**

[1]The idea of doing reconnaissance for the purpose of pen testing or malicious activity through google hacking, has

already reached levels of automation – the problem is how the threat gets often neglected by those that actually

suffer from a breach later on. I came across to an [2]article pointing out that :

*" Anyone who wants to hack into sensitive information on New Zealand internet sites might be pleased to know it can be as easy as typing keywords into a Google search. Researchers at Massey University's Albany campus say the*

*country's websites are more vulnerable to "Google hacking" than anywhere else in the world. University Information and Mathematical Sciences Institute senior lecturer Dr Ellen Rose and graduate student Natalia Nehring recently*

*completed a study into the topic. "*

Not exactly a type of [3]cyberterrorism exercise such as the most recent [4]DigitalStorm, but it's logical to con-



clude that if someone takes the time and effort to data mine the web, localize the attack like in this case, a lot will be revealed. In a recent article, CSOonline goes in-depth into the [5]security implications posed by Google. I once had a

[6]chat with [7]Johnny Long on many topics, among the "few", of course, was google hacking. He made a good point on saying that it's whatever you actually do with the results that matters most, and how diverse is the threat – by

googling your lights off for instance.

What you should keep in mind is that it isn't Google to blame, the way "[8]Improving the Security of Your Site

by Breaking Into it" provoked awareness, and not damage. Think the problem isn't big of a shot – gather some

intelligence by yourself through the [9]Google Hack Honeypot project.

1. [http://static.flickr.com/38/77978160\\_b165c9d377.jpg](http://static.flickr.com/38/77978160_b165c9d377.jpg)
2. <http://www.stuff.co.nz/stuff/0,2106,3676220a11,00.html>
3. <http://ddanchev.blogspot.com/2006/05/techno-imperialism-and-effect-of.html>
4. [http://www.washingtontechnology.com/news/1\\_1/daily\\_news/27877-1.html](http://www.washingtontechnology.com/news/1_1/daily_news/27877-1.html)
5. [http://www.csoonline.com/read/050106/google\\_security.html](http://www.csoonline.com/read/050106/google_security.html)
6. <http://www.astalavista.com/media/archive1/newsletter/issue>

[\\_25\\_2006.pdf](#)

7. <http://johnny.ihackstuff.com/>
8. <http://nsi.org/Library/Compsec/farmer.txt>
9. <http://ghh.sourceforge.net/>

328

### **Espionage Ghosts Busters (2006-05-23 18:35)**

In previous posts, "[1]Insider Competition in the Defense Industry", and "[2]The anti virus industry's panacea - a virus recovery button", I gave examples of insider trading, of [3]malware infecting border-screening computers, or the

plain truth on how U.S "manufactured" PCs are actually assembled in China these days.

Obviously, plain old [4]paranoia without solid background still dominates as " *Representative Frank Wolf (R-VA) has announced that the State Department has agreed not to use 900 computers purchased from Chinese-owned*

*Lenovo on classified computer networks. The US-China Commission, a bipartisan congressional commission, raised*

*concerns when State announced the purchase of 16,000 desktop computers from Lenovo, with 900 to be used*

*on secret networks connected to the Defense Department's classified [5]SIPRnet (Secret Internet Protocol Router*

*Network). State is changing its procurement process to better track changes in vendor ownership that could impact*

*national security. "*

There's a common myth that a nation's military uses a specially dedicated networks, ones greatly differing from the standard OSI model the way we know it - which is wrong as it would limit the usability, and increase the costs of operating. My point is that, even a PC sold by Dell would eventually run a Microsoft OS, thus exposing it to the monocultural insecurity by itself, and the [6]human weaknesses of the person operating the PC itself, not guarding the SIPRnet perimeter.

It would be easier for Chinese hackers or government entities to take advantage of client side attacks on any of these systems, then to ship them backdoor-ready risking too much in case of possible espionage fiasco. There have been known cases of malware leaking nuclear plant information, or [7]employees P2Peering sensitive/classified information. Be it, [8]hardware keyloggers, [9]logic bombs, [10]BIOS rootkits, given the scrutiny, even a slight ambiguation might have vanished in the air. [11]Modern spy gadgets are evolving, [12]espionage cases are still happening and some get even public, but in case you're interested in the true [13]ghost covert operative - stay tuned for the Stand Alone Complex Novel!

1. <http://ddanchev.blogspot.com/2006/05/insider-competition-in-defense.html>

2. <http://ddanchev.blogspot.com/2006/04/anti-virus-industrys-panacea-virus.html>
3. <http://www.wired.com/news/technology/0,70642-0.html>
4. [http://www.gcn.com/online/vol1\\_no1/40811-1.html](http://www.gcn.com/online/vol1_no1/40811-1.html)
5. <http://en.wikipedia.org/wiki/SIPRNet>
6. [http://www.windowsecurity.com/articles/Reducing\\_Human\\_Factor\\_Mistakes.html](http://www.windowsecurity.com/articles/Reducing_Human_Factor_Mistakes.html)
7. [http://www.theregister.co.uk/2006/05/17/japan\\_power\\_plant\\_virus\\_leak/](http://www.theregister.co.uk/2006/05/17/japan_power_plant_virus_leak/)
8. <http://www.keyghost.com/>
9. [http://en.wikipedia.org/wiki/Logic\\_bomb](http://en.wikipedia.org/wiki/Logic_bomb)
10. [http://www.ngssoftware.com/jh\\_bhf2006.pdf](http://www.ngssoftware.com/jh_bhf2006.pdf)
11. [http://www.forbes.com/technology/2006/04/15/intelligence-spying-gadgets\\_cx\\_lh\\_06slate\\_0418tools.html](http://www.forbes.com/technology/2006/04/15/intelligence-spying-gadgets_cx_lh_06slate_0418tools.html)
12. <http://ddanchev.blogspot.com/2006/02/top-level-espionage-case-in-greece.html>
13. <http://www.cyberpunkreview.com/graphic-novels/gits-stand-alone-complex-graphic-novel-may-24th>

329

**Arabic Extremist Group Forum Messages'  
Characteristics (2006-05-23 18:56)**

Ever wondered what's the font size of a terrorist forum posting? These guys are really deep into using AI for gathering

intelligence on various [1]Cyberterrorism threats, and as you can see they neatly [2]visualize their [3]findings.

"[4]Applying Authorship Analysis to Extremist-Group Web Forum Messages" by Ahmed Abbasi and Hsinchun Chen,

University of Arizona seem to have found a way, or at least patters of ongoing terrorist communication, and of course propaganda online. What they did was :

*" To explore these problems, we modified an existing framework for analyzing online authorship and applied it to Arabic and English Web forum messages associated with known extremist groups. We developed a special multilingual model—the set of algorithms and related features—to identify Arabic messages, gearing this model toward the language's unique characteristics. Furthermore, we incorporated a complex message extraction component to allow the use of a more comprehensive set of features tailored specifically toward online messages. A series of experiments evaluating the models indicated a high level of success in identifying communication patterns. "*

[5]Social network analysis has a lot of potential, and with [6]data mining it seems to be the perfect match for

the recent trouble with [7]NSA's domestic spying program. [8]DearNSA.com and the [9]Patriot Search are aiming to

solve the problem for both parties – efficiently.

There's a lot of propaganda chat going on online all the time, and among the very few limitations that bother

me about such web aggregation of open source information are the use of steganography, or plain-simple Dark Web

(closed for crawlers with basic/sophisticated authentication in place) communication – remember there's a lot of

noise to sort out through as well.

1. <http://ddanchev.blogspot.com/2006/05/techno-imperialism-and-effect-of.html>
2. <http://ddanchev.blogspot.com/2006/03/visualization-in-security-and-new.html>
3. <http://ai.arizona.edu/research/terror/publications/conf/SeminarGroupAuthorship.pdf>
4. <http://ai.arizona.edu/go/intranet/papers/Final.pdf>
5. <http://ddanchev.blogspot.com/2006/05/terrorist-social-network-analysis.html>
6. <http://ddanchev.blogspot.com/2006/03/data-mining-terrorism-and-security.html>

7.

[http://en.wikipedia.org/wiki/NSA\\_warrantless\\_surveillance\\_controversy](http://en.wikipedia.org/wiki/NSA_warrantless_surveillance_controversy)

8. <http://www.dearnsa.com/>

9. <http://ddanchev.blogspot.com/2006/01/still-worry-about-your-search-history.html>

330

### **The Current, Emerging, and Future State of Hacktivism (2006-05-23 19:06)**

[1]Zone-H recently reported yet another major [2]hacktivism case in what's stated to be [3]the biggest hacking

incident in the web-hosting history- single hack, multiple targets exposed and their audiences' attention "acquired".

The very same type of tension happened several weeks ago due to the [4]Muhammad cartoons. It may seem

questionable whether [5]Hacktivism would survive in today's for-profit online crime world, but discussion and

execution opens up new boundaries the way the author of this research did.

I feel I went through what's perhaps the most recent and extensive research done on Hacktivism, "[6]Hack-

tivism and the Future of Political Participation" by [7]Alexandra Samuel - a perfect moment to mention the [8]daily updated security resources, that I go through instantly, hundreds more will soon be shared as well!

The dissertation " *looks at the phenomenon of hacktivism: the marriage of political activism and computer hacking.*

*It defines hacktivism as the nonviolent use of illegal or legally ambiguous digital tools in pursuit of political ends.*

*Those tools include web site defacements, redirects, denial-of-service attacks, information theft, web site parodies, virtual sit-ins, virtual sabotage, and software development. The dissertation uses data from fifty-one interviews in conjunction with additional primary and secondary source material. This data is used to construct a taxonomy of*

*hacktivism, and apply the taxonomy to three core issues in political participation. "*

The big picture, the details, and everything in between, how fast can you print, bind and read this masterpiece?

1.

<http://photos1.blogger.com/blogger/1933/1779/1600/hacktivism.2.jpg>

2. <http://ddanchev.blogspot.com/2006/02/hacktivism-tensions.html>

3. <http://www.zone-h.com/en/news/read/id=206009/>

4. <http://cryptome.org/muhammad.htm>

5. <http://en.wikipedia.org/wiki/Hacktivism>

6. <http://www.alexandrasamuel.com/20060510/now-available-hacktivism-the-future-of-political-participation>

7. <http://www.alexandrasamuel.com/>

8. <http://del.icio.us/DDanchev/>



## **Bedtime Reading - The Baby Business (2006-05-23 19:15)**

While not necessarily an [1]AI, a [2]Project 2501 type of living entity breakthrough development, there's a growing

(underground) market for genetically modified newborns, a scary scenario that reminds of previous [3]episodes

(Criminal Nature) of [4]the Outer Limits and of course [5]Gattaca in all of its twisted beauty and utopian representa-

tion of Space as the "final destination".

[6]The Baby Business [7]explains [8]how parents willing to pay to make their kids "better" are actually fueling growth in the market itself. What's a "better" kid anyway? One that's smart, beautiful, that thinks like an Ivy League freshman when its 10 years old - is it thinking or theoritizing? - a math genius with a second life of a marketer?

Or intelligent, passionate about something eventually becoming a turning point for his future development,

realizing admitting and getting over failure, being interested instead of being interesting type of kid, with a pure

feeling of self-development and self-realization? - a soul.

Would the "haves" donate genetic know-how, or would one be eventually found and commercialized? I think

utopias are a powerful driving force, yet perfection remains among the biggest human weaknesses ever - [9]super-

human is a state of mind if you are willing to embrace it.

1. <http://www.blogcharm.com/AI/>
2. [http://en.wikipedia.org/wiki/Project\\_2501](http://en.wikipedia.org/wiki/Project_2501)
3. <http://www.theouterlimits.com/downloads/index.html?controlvoices>
4. <http://ddanchev.blogspot.com/2006/02/dvd-of-weekend-outer-limits-sex-and.html>
5. <http://en.wikipedia.org/wiki/Gattaca>
6. <http://www.amazon.com/gp/product/1591396204/103-4695307-7340639?v=glance&n=283155>
7. [http://www.hbs.edu/news/021506\\_spar.html](http://www.hbs.edu/news/021506_spar.html)
8. <http://www.genetics-and-society.org/newsdisp.asp?id=990>
9. <http://en.wikipedia.org/wiki/Overman>

332

### **Travel Without Moving - Korean Demilitarized Zone (2006-05-27 19:51)**

[1]Continuing the [2]travel without moving series, the [3]Korean Demilitarized Zone remains a [4]hot spot with

[5]North Korea publicly stating its ambitions of joining the nuclear club. How big of a threat is the statement anyway?

I believe it's a desperate move from the North Koreans' side, while trying to put itself on the world's map again - and

the news of course.

What they lost was the momentum, one that Iran greatly took advantage of. Think about it, as the U.S's War

on Terror is like any "product concept", it inevitably passes through introduction, growth, maturity and decline stages in respect to public relations. [6] Abu Ghraib's offensive PSYOPS case, a national disaster in between, Muhammad's

cartoons, and NSA's fiasco seemed to further strengthen the momentum of announcing [7] their intentions without

fear of having the U.S in their backyard – smart move fully taking advantage of the situation and definitely resulting

in a future diplomatic solution.

While North Korea is presumably hoping to improve the nation's dignity and reputation as scientifically sophisti-

cated enough to be recognized, building nuclear weapons when the central statistical bureau releases reports of

people dying out of starvation reminds of the best Cold War strategy game scenario I ever played.

No real army for the regime, but sneaky partisans everywhere, no roads, no buildings, but nuclear bombs and

cruise missiles in every city, as well as income distribution model based on the "model of leftovers", thus, riots and lack of any production capabilities. I remember watching a documentary where a soldier was trying to broadcast

over the border, and of course, North Korea's jammers in action. Censoring news, obsessive self-regulation practices,

total denial of problems, and keeping everyone in a twisted reality for as long as necessary is a daily practice – still, there are [8]capitalists trying to operate business ventures there.

What the international community could possibly do is not to lose touch with these people, and constantly

"ping" their diplomacy while trying to achieve bargain deals – the problem is that even Asian countries find North Korea a spooky place. [9]Kim Jong-il is not a mad man, but a man looking for attention, give him some without having

him "envision" a [10]conventional weaponry phrase in his country's history.

1.  
[http://photos1.blogger.com/blogger/1933/1779/1600/North\\_Korea\\_Border.jpg](http://photos1.blogger.com/blogger/1933/1779/1600/North_Korea_Border.jpg)
2. <http://ddanchev.blogspot.com/2006/05/travel-without-moving-scratching-floor.html>
3. [http://en.wikipedia.org/wiki/Korean\\_Demilitarized\\_Zone](http://en.wikipedia.org/wiki/Korean_Demilitarized_Zone)
4.  
<http://maps.google.com/maps?f=q&hl=en&q=north+korea+Joint+Security+Area&t=k&map;om=1&ll=37.956287,126.677481&spn=0.006362,0.009978>
5.  
[http://en.wikipedia.org/wiki/North\\_Korea\\_nuclear\\_weapons\\_program](http://en.wikipedia.org/wiki/North_Korea_nuclear_weapons_program)

6. <http://yro.slashdot.org/article.pl?sid=04/11/07/1442217>
7. [http://en.wikipedia.org/wiki/Iran\\_and\\_weapons\\_of\\_mass\\_destruction](http://en.wikipedia.org/wiki/Iran_and_weapons_of_mass_destruction)
8. <http://www.forbes.com/business/global/2006/0227/046A.html>
9. [http://en.wikipedia.org/wiki/Kim\\_Jong\\_Il](http://en.wikipedia.org/wiki/Kim_Jong_Il)
10. <http://news.google.com/news?hl=en&ned=us&q=north+korea%2Bnuclear&ie=UTF-8&scoring=d>

333

### **Aha, a Backdoor! (2006-05-27 20:19)**

Security precautions can indeed blur the transparency of a company's financial performance – one that's extremely

important in the post-Enron corporate world. Under fire over some of the biggest corporate scandals during the last

decade, the Securities and Exchange Commission (SEC) has been trying to [1]change the data standards to ensure

greater accountability and support decision makers. On the other hand, the U.S's Intelligence Czar, John Negroponte

remains in position to "exempt" publicly traded companies from reporting matters in relation to nothing else but national security.

From the [2]article :

*" Now, the White House's top spymaster can cite national security to exempt businesses from reporting requirements President George W. Bush has bestowed on his intelligence czar, John Negroponte, broad authority, in the name of national security, to excuse publicly traded companies from their usual accounting and securities-disclosure obligations. Notice of the development came in a brief entry in the Federal Register, dated May 5, 2006, that was opaque to the untrained eye. "*

What the U.S government gets is stimulated to [3]invest in homeland security publicly traded companies, given the

benefits of the possible "exemption" and countless opportunities for profitable speculation. If the backdoor left gets used for purposes other than classifying some obvious defense contractors' accounting histories I wouldn't doubt

seeing Coca Cola diversifying to take advantage of expanding the unaccountable R &D department. Moreover, today

I came across to an independent research stating that [4]classified and unaccountable military spending is at its peak.

It's fascinating to label something as top secret and let the world know about it 30 years later in order to lose

the public effect of the discovery, still "excusing" companies to fuel growth would open up a great deal for corporate fraud schemes, but yes, investments too.

1. <http://www.vnunet.com/financial-director/analysis/2156747/standard-issue>
2. <http://msnbc.msn.com/id/12952860/>
3. <http://www.redherring.com/article.aspx?a=16929>
4. <http://www.realcities.com/mld/kwashington/14623031.htm>

334

### **Forgotten Security (2006-05-27 20:35)**

It's one thing to [1]expose a Pengaton conference's attendees list, and another Mr. Blair's security plans intended to

protect the Prime Minister from a terrorist attack during the Labour Party conference".

From the [2]article :

*" Security plans intended to protect the Prime Minister from a terrorist attack during the Labour Party conference have been left in a hotel. The documents include a list of ways in which Mr Blair and members of his Cabinet could be killed as they attend the five-day conference at Manchester's G-Mex Centre in September. Greater Manchester Police*

*said that the dossier, found at the Midland Hotel, had been left by a member of hotel staff but insisted that the plans were not secret. "*

Every country has it's reputable think tanks, whether representing PhDs' with eyeglasses thick enough to have

the sun burn their eyes, or plain simple analysts, worst case scenarios when protecting national leaders are among

the top priorities. I think that even if the plans weren't secret, they reveal a lot of info on the security agency's

thinking and hypotizing approach, still, no advantage could have been taken given the short timeframe – thankfully.

1. <http://www.washingtonpost.com/wp-dyn/content/article/2006/05/09/AR2006050901725.html>

2. <http://uk.news.yahoo.com/25052006/356/blair-s-secret-security-plans-found-hotel.html>

335

### **Delaying Yesterday's "0day" Security Vulnerability (2006-05-27 20:47)**

[1]I never imagined we would be waiting for the release of a "0day" vulnerability, but I guess that's what happens if you're not a customer of an infomediary in the growing [2]market for software vulnerabilities – growth in respect to,

researchers, infomediaries and security vulnerabilities. Stay tuned for "[3]Exploit Of Windows 2000 Zero-day To Hit In June", and take your time to appreciate that it's affecting "extended support" software. From the article :

*" Symantec warned its enterprise customers Thursday that an unpatched vulnerability in Windows 2000's file*

*sharing protocol has surfaced, with details of an exploit expected to show next month. According to the Cupertino,*



*Calif. company's alert, an exploit for the zero-day bug in Windows 2000's SMB (Server Message Block) protocol has been created by Immunity Security, the makers of the CANVAS exploit-creation platform. By Immunity researcher Dave Aitel's account, the exploit leverages a flaw in the operating system's kernel that can be triggered through SMB, and will give an attacker full access to the PC. Aitel claimed Immunity will make the exploit public in June. "Immunity is considered to be a reliable source and we are of the opinion that this information should be treated as fact," read Symantec's warning. "An official security update from Microsoft will likely not be in development until after June when the information is released. "*

Well, how can they fix in such a way, even though their "sophisticated", quality-obsessed [4]patch management practices. When working with vulnerabilities, or updating yourself with the dailypack of new ones, don't live with the false feeling of their uniqueness, but try figuring out how to be a step ahead of the vulnerabilities management stage. If Microsoft requested from Immunity Security to look up for possible security vulnerabilities, gave them a deadline, and secured a commission in case a vulnerability is actually found, it would have perfectly fited in the scenario in a previous post "[5]Shaping the Market for Security Vulnerabilities Through Exploit Derivatives" - [6]reporting a vulnerability, let's not mention web application vulnerability is for the brave these days. Moreover,

"[7]Economic Analysis of the Market for Software Vulnerability Disclosure" quotes Arora et al. on the same issue from a vendor's point of view :

*" developing an economic model to study a vendor's decision of when to introduce its software and whether or not to patch vulnerabilities in its software. They compare the decision process of a social-welfare maximizing monopolistic vendor, to that of a [8]profit-maximizing monopolistic vendor. Interestingly, they observe that the profit-maximizing vendor delivers a product that has fewer bugs, than a social-welfare maximizing vendor. However, the profit-maximizing vendor is less willing to patch its software than its social-welfare maximizing counterpart. " -*

[9]The Price of Restricting Vulnerability Publications is indeed getting higher.

Reactive, Proactive, or Adaptive - what's your current [10]security strategy?

1.  
<http://photos1.blogger.com/blogger/1933/1779/1600/exploited.jpg>
2. <http://ddanchev.blogspot.com/2005/12/0bay-how-realistic-is-market-for.html>
3. <http://www.techweb.com/wire/security/188500133>
4.  
<http://www.microsoft.com/technet/community/columns/secmgmt/sm0506.mspx>

5. <http://ddanchev.blogspot.com/2006/05/shaping-market-for-security.html>

6. <http://www.cerias.purdue.edu/weblogs/pmeunier/policies-law/post-38>

336

7. <http://csdl.computer.org/comp/proceedings/hicss/2004/2056/07/205670180a.pdf>

8. <http://ddanchev.blogspot.com/2006/03/5-things-microsoft-can-do-to-secure.html>

9. [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=874846](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=874846)

10. <http://ddanchev.blogspot.com/2006/05/valuing-security-and-prioritizing-your.html>

337

### **Who's Who in Cyber Warfare? (2006-05-28 15:34)**

Wondering what's the current state of cyber warfare capabilities of certain countries, I recently finished reading a

report "[1]Cyber Warfare: An Analysis of the Means and Motivations of Selected Nation States", a very in-depth summary of Nation2Nation Cyber conflicts and developments I recommend you to read in case you're interested. It

covers China, India, Iran, North Korea, Pakistan, and, of course, Russia. Some selected brief excerpts on China, Iran,

and Russia :

## **China**

*" Beijing's intelligence services continue to collect science and technology information to support the government's goals, while Chinese industry gives priority to domestically manufactured products to meet its technology needs. The PLA maintains close ties with its Russian counterpart, but there is significant evidence that Beijing seeks to develop its own unique model for waging cyber warfare. "*

## **Iran**

*" The armed forces and technical universities have joined in an effort to create independent cyber R & D centers and train personnel in IT skills; and second, Tehran actively seeks to buy IT and military related technical assistance and training from both Russia and India. "*

## **Russia**

*" Russia's armed forces, collaborating with experts in the IT sector and academic community, have developed a robust cyber warfare doctrine. The authors of Russia's cyber warfare doctrine have disclosed discussions and debates concerning Moscow's official policy. "Information weaponry," i.e., weapons based on programming code, receives paramount attention in official cyber warfare doctrine. "*

Technology as the next Revolution in Military Affairs (RMA) was inevitable development, what's important to

keep in mind is knowing who's up to what, what are the foundations of their military thinking, as well as who's

copying attitude from who. Having the capacity to wage offensive and defense cyber warfare is getting more

important, still, military thinkers of certain countries find [2]network centric warfare or total renovation of [3]C4I

communications as the panacea when dealing with their about to get scraped conventional weaponry systems.

Convergence represents countless opportunities for waging Cyber Warfare, offensive one as well, as I doubt there

isn't a country working on defensive projects.

In a previous post [4]Techno-Imperialism and the Effect of Cyberterrorism I also provided detailed overview of

the concept and lots of real-life scenarios related to Cyberterrorism, an extension of Cyber warfare capabilities. It

shouldn't come as a surprise to you, that a nation's military and intelligence personnel have, or seek to gain access

to 0day security vulnerabilities, the currency of trade in today's E-society as well as recruiting local "renegades".

338

Undermining a nation's confidence in its own abilities, the public's perception of inevitable failure, sophisticated [5]PSYOPS, "excluded middle" [6]propaganda, it all comes down to who's a step ahead of the event by either predicting or intercepting its future occurrence. Information is not power, it's noise turning into Knowledge, one that

becomes power – if and when exercised.

1. <http://www.ists.dartmouth.edu/directors-office/cyberwarfare.pdf>
2. [http://www.vodium.com/MediapodLibrary/index.asp?library=dod\\_ofc\\_incw&SessionArgs=0A1U0000000100000111](http://www.vodium.com/MediapodLibrary/index.asp?library=dod_ofc_incw&SessionArgs=0A1U0000000100000111)
3. [http://en.wikipedia.org/wiki/Command,\\_control,\\_and\\_communications](http://en.wikipedia.org/wiki/Command,_control,_and_communications)
4. <http://ddanchev.blogspot.com/2006/05/techno-imperialism-and-effect-of.html>
5. [http://www.theregister.co.uk/2005/12/13/russia\\_today\\_tv\\_station\\_hack/](http://www.theregister.co.uk/2005/12/13/russia_today_tv_station_hack/)
6. <http://www.cjr.org/issues/2006/3/schulman.asp>

339

### **No Anti Virus Software, No E-banking For You (2006-05-30 17:33)**

[1]Malware and [2]Phishing are the true enemies of E-commerce, its [3]future penetration, and [4]E-banking

altogether. Still, there are often banks envisioning the very basic risks, and hedging them one way or another, as

"[5]Barclays gives anti-virus software to customers"

" *Barclays Bank is issuing UK internet banking customers with anti-virus software, as part of attempts to re-*

*duce online identity theft. The bank has signed a deal with Finnish anti-virus firm F-Secure, which will provide*

*software to the bank's 1.6m UK internet banking customers. While other banks offer discounted anti-virus software*

*deals to customers, Barclays is the first in the UK to give it away for free. 'Nearly two-thirds of home PCs don't have active virus protection, and one in five is actually infected by a virus, placing people at risk from data theft, as well as damage to their computers,' said Barnaby Davis, director of electronic banking at Barclays. "*

I find the idea a very good mostly because compared to other banks that try to [6]reestablish the email com-

munication with their customers, but starting from the basics, you can't do E-banking without generally acceptable

security measure in place. And while an [7]AV solution doesn't necessarily mean the customer wouldn't get attacked

by other means, or that it would be actually active in the moment of the attack, this is a very smart to do. To take

advantage of even more benefits, Barclays must actively communicate their contribution and unique differentiating

point to their customers, in comparison with the other banks - it's getting harder for companies to retain customers

due to improved access to information, thus more informed decisions.

You can't just deal with the technological part of the problem, but avoid the human side in it, as education

and awareness will result in less gullible, but more satisfied and longer retained customers. Phishing is today's

efficient social engineering, and a bank's site shouldn't be assumed "secure" as on many occasions site-specific vulnerabilities improve the truthfulness of the scam itself. Forwarding the responsibility for secured access to the

E-banking feature to final customers should be simultaneous with the bank auditing its web services. In the up-

coming years, with the rise of [8]mobile banking, I think we will inevitably start seeing more mobile phishing attempts.

Ebay's PayPal is still a major player in online payments, on its way to dominate [9]mobile payments too. The

trend and potential of [10]cross-platform malware is what both AV vendors and payment providers should keep in

mind.

1. <http://ddanchev.blogspot.com/2006/01/malware-future-trends.html>

2. <http://ddanchev.blogspot.com/2006/03/anti-phishing-toolbars-can-you-trust.html>

3. <http://ddanchev.blogspot.com/2006/01/hidden-internet-economy.html>

4. <http://ddanchev.blogspot.com/2006/01/security-threats-to-consider-when.html>

5. <http://www.computing.co.uk/computing/news/2157044/barclays-gives-anti-virus>

6. <http://ddanchev.blogspot.com/2006/04/heading-in-opposite-direction.html>



7. <http://ddanchev.blogspot.com/2006/01/why-relying-on-virus-signatures-simply.html>
8. <http://upetd.up.ac.za/thesis/available/etd-07202004-111814/unrestricted/00dissertation.pdf>
9. [http://www.paymentsnews.com/2006/04/paypal\\_releases.html](http://www.paymentsnews.com/2006/04/paypal_releases.html)
10. <http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=111435>

340

### **Microsoft in the Information Security Market (2006-05-30 17:51)**

[1]Microsoft is emptying its pockets with tiny acquisitions of security solution providers with the idea to target the

masses in its [2]all-in-one security service [3]OneCare. There's nothing wrong with offering up to three licenses for

\$49.95 per year, at least not from a marketing point of view.

[4]Microsoft's Security Ambitions are getting huge " *as it continues to reveal its security ambitions in very obvious ways. Its \$75 million acquisition of SSL VPN vendor Whale Communications last week shows just how deep it wants to go against the established leaders of various security*

*technologies. Already in Microsoft's security sights are the antivirus and antispymware vendors. Since buying European antispymware vendor Giant Company Software and antivirus vendor Sybari, it was pretty clear that Microsoft intended*

*to get into the malware protection market. Symantec, McAfee and Trend Micro seemed to be the clearest targets, but so are Sophos, CA, F-Secure and scores more smaller vendors. "*

Competition is always good for all parties involved. In another article on the topic, WebRoot's founder, a lead-

ing anti-spyware solutions provider, gave [5]great comments about Microsoft's take over of the infosec market : "*The taking of a second-best product in this space is akin to locking half the doors in your house," he said. "Vista will not solve the spyware problem. It may change the vector of attack, but it will not solve this problem. And I'll bet the company on it. "*

Microsoft really surprised me with their release of the [6]Strider Honey Monkeys Crawler, as precisely the

type of in-house research that would act as a main differentiation point of its solutions. The problem has never been

the technology, they still have some of the [7]brightest minds in the world working for them, but providing value

and communicating the idea to the final customer. Security as a second priority isn't tolerated by customers, and

Microsoft is last company that the end user associates with security. Obsessed with perfection, and still living in the

product marketing concept world, is outdated thinking, the way pushing features based on "what the sample says"

is not going to hold the front any longer. Customers beg to participate!

While for the time being Microsoft is rediscovering the Web, and working on Vista, money doesn't necessarily

buy innovation, prone to make impact individuals do -ones heading to [8]Mountain View, California where the real

action is.

1. <http://ddanchev.blogspot.com/2006/03/5-things-microsoft-can-do-to-secure.html>

2. [http://www.pcworld.com/reviews/article/0,aid,125817,tk,soc\\_digg,pg,1,00.asp](http://www.pcworld.com/reviews/article/0,aid,125817,tk,soc_digg,pg,1,00.asp)

3. <http://www.geek.com/news/geeknews/2006May/gee20060530036469.htm>

4. <http://internetweek.cmp.com/news/188100960;jsessionid=5K4XNF1ZZTX3OQSNDBGCKHSCJUMKJVN>

5. <http://www.ecommercetimes.com/story/50669.html>

6. <http://research.microsoft.com/HoneyMonkey/>

7. <http://www.forbes.com/forbes/2005/1031/045.html>

8. [http://en.wikipedia.org/wiki/Mountain\\_View,\\_Santa\\_Clara\\_County,\\_California](http://en.wikipedia.org/wiki/Mountain_View,_Santa_Clara_County,_California)

## **Covert Competitive Intelligence (2006-05-30 18:03)**

Yet another agreement on alleged [1]covert competitive intelligence, [2]this time, " *Westjet Airlines says it's sorry that members of its management team covertly accessed a confidential Air Canada website, and has agreed pay \$15.5*

*million. In a joint news release from the two carriers, Westjet said that in 2003-2004, members of their management*

*team "engaged in an extensive practice of covertly accessing a password protected proprietary employee website*

*maintained by Air Canada to download detailed and commercially sensitive information without authorization or consent from Air Canada. "*

It's worth noting that Air Canada was actually aware of the [3]security event, knew [4]when it happened, and

managed to trace it back to their competitors. Today's competitive intelligence does include unethical information

gathering whether in-house, or "outsourced" practices, as [5]DDoS for hire still make the headlines, compared to the many other still undetected [6]insider leakages years ago. It's also impressive [7]how [8]Dumpster diving still

remains a serious threat - so make sure you [9]shred your secrets!

1. <http://ddanchev.blogspot.com/2006/05/insider-competition-in-defense.html>

2.

[http://www.ctv.ca/servlet/ArticleNews/story/CTVNews/20060529/westjet\\_apology\\_060529/20060529?hub=CTVNewsAt1](http://www.ctv.ca/servlet/ArticleNews/story/CTVNews/20060529/westjet_apology_060529/20060529?hub=CTVNewsAt1)

1

3. <http://ddanchev.blogspot.com/2006/02/detecting-intruders-and-where-to-look.html>

4. <http://ddanchev.blogspot.com/2006/04/digital-forensics-efficient-data.html>

5. <http://www.csoonline.com/read/050105/extortion.html>

6. <http://ddanchev.blogspot.com/2005/12/insiders-insights-trends-and-possible.html>

7. <http://www.crime-scene-investigator.net/DumpsterDiving.pdf>

8. [http://en.wikipedia.org/wiki/Dumpster\\_diving](http://en.wikipedia.org/wiki/Dumpster_diving)

9. <http://www.fellowes.com/tools/shreddersshowcase/>

342

## **The Global Security Challenge - Bring Your Know-How (2006-05-30 18:16)**

It's a public secret that the majority of innovative ideas come from either the academic environment, or plain simple

entrepreneurial spirits. I find such annual competitions as a valuable incentive for both sides to unleash the full

power of their ideas, or commercialize them - consciously or subconsciously. [1]SpaceShipOne is a case study on how

[2]elephants can't dance, or at least how they dance on high profit margins only.

Recently announced, [3]The Global Security Challenge seeks *"..to help young startups succeed in the security*

*field. Take advantage of this unique opportunity to get your ideas in front of investors, media, and government and*

*industry leaders. "* And most importantly :

*"We seek to uncover the creative capabilities of innovators in universities and infant companies that apply to*

*public security needs. This includes software, hardware or other industrial solutions that help (a) protect people,*

*critical infrastructure, facilities and data/electronic systems against terrorist or other criminal attacks and natural disasters or (b) help governments, businesses and communities defend against, cope with or recover from such*

*incidents. Examples of Technologies We Seek:*

- *Mesh Networks*
- *Data Storage and Recovery*
- *Detection/ Sensors*
- *Biometrics*
- *Search Software*
- *Cyber/Network Security*
- *Communications Interoperability & Reconstruction*

- *Biological/Chemical/Radiological Remediation*
- *Protective Equipment*
- *RFID, Asset Tracking & Container Security*
- *Biotechnology*

I bet [4]Europe's Top Private Security Companies revenues' exceed the limit of having less than £ 10 million in

annual revenues, it's worth speculating on their participation. Do your homework, know your competitors better

than they do themselves, work out your elevator pitch, and disrupt.

As far as acquisitions are concerned, [5]SiteAdvisor is the first recently acquired startup that comes to my mind

with its [6] \$70M acquisition deal valuation. As it obviously goes beyond VC type of mentorship, to many this seemed

as an overhyped deal. There's no price for being a pioneer, but a price on acquiring the position – a stairway to

heaven. Right now, a [7]vertical security market segment is slowly developing, and it is my humble opinion that the

company's pioneering position is poised for success. Another alternative to SiteAdvisor's [8]safe search function is

the [9]recently launched [10]Scandoo.com which actually integrates the results from Google and Yahoo – I doubt

users would that easily change their search preferences though.

Who's next to get acquired, or hopefully [11]funded?

1. <http://en.wikipedia.org/wiki/SpaceShipOne>
2. <http://www.amazon.com/gp/product/0060523794/103-2488219-6696641?v=glance&n=283155>
3. <http://www.globalsecuritychallenge.com/>
4. <http://www.redherring.com/Article.aspx?a=15436&hed=Top+Private+Security+Companies>
5. <http://ddanchev.blogspot.com/2006/04/spotting-valuable-investments-in.html>
6. <http://sunbeltblog.blogspot.com/2006/05/oh-and-while-were-on-subject-of.html>
7. <http://www.redherring.com/Article.aspx?a=17031&hed=Melding+Search+and+Security&sector=Industries&subsector=>

[InternetAndServices](#)

343

8. [http://www.siteadvisor.com/studies/search\\_safety\\_may2006.html](http://www.siteadvisor.com/studies/search_safety_may2006.html)
9. [http://home.businesswire.com/portal/site/google/index.jsp?ndmViewId=news\\_view&newsId=20060522005802&newsLanguage=en](http://home.businesswire.com/portal/site/google/index.jsp?ndmViewId=news_view&newsId=20060522005802&newsLanguage=en)
10. <http://www.scandoo.com/>



11.

<http://www.globalsecuritychallenge.com/enter/index.html>

344

### **Healthy Paranoia (2006-05-31 15:40)**

More developments on the US-China Commission's decision not to use Chinese manufactured PCs on the SIRPnet

follow, an event I covered in a previous post "[1]Espionage Ghosts Busters". The official stated [2]attack vector, namely that ". . . *a significant portion*" of *Lenovo* is owned by the Chinese Academy of Sciences, an arm of the Chinese government. " is nothing more than a [3]healthy paranoia to me, one reaching to the skies on certain occasions, of course. Just came across to an [4]article summarizing some recent events :

*" The U.S. State Department recently declared that due to national security concerns, it would restrict use of*

*the 16,000 computers it purchased to nonclassified work. It had originally planned to use 900 of the machines on a*

*network connecting U.S. embassies. Lenovo's goal of becoming the "Sony of China" could be impeded by worries over*

*its machines' security, blocking its strategy to move out of its Asia stronghold and into the West by courting North American computer users and possibly listing on U.S. stock markets. That realization sparked outcry from officials of both the Chinese government and the computer company. "*

However, today's [5]monocultural reality, and favorable trend towards [6]diversity will have greater impact on

the (in) security of the PCs. Moreover, the "manufactured in China" reality is a commonly shared myth, one that keeps getting debunked as well :

*" Almost any PC you can name has Chinese content," said Roger Kay, president of the research firm Endpoint*

*Technologies Associates. He pointed to Intel semiconductors and Seagate hard drives made in China. He also noted*

*that 80 percent of notebooks sold worldwide are manufactured in China. "*

Even if Lenovo dared to implement hardware backdoors, or ship the PCs rootkit ready, it could have success-

fully ruined its business future - [7]insider pressure is always an option, but what do you got besides speculation?

Don't unload China Communist Party's load on this recently separated from IBM division, they aren't in the most

favorable position, still remain among the top players on the PC market, right next to the efficiency machine Dell,

which as a matter of fact recently completed its [8]second high-tech factory in China.

Healthy paranoia, or the George Orwell inside you? Comic page text generated at [9]Gaxed.com

1. <http://ddanchev.blogspot.com/2006/05/espionage-ghosts-busters.html>
2. <http://www.msnbc.msn.com/id/12861245/>
3. [http://www.fas.org/irp/congress/2005\\_hr/hhrg109-58.html](http://www.fas.org/irp/congress/2005_hr/hhrg109-58.html)

4. [http://redherring.com/Article.aspx?  
a=17039&hed=Lenovo%2c+Chinese+Lash+Out](http://redherring.com/Article.aspx?a=17039&hed=Lenovo%2c+Chinese+Lash+Out)
5. [http://www.computerworld.com.au/index.php/id;186487648  
9;fp;2;fpid;3](http://www.computerworld.com.au/index.php/id;1864876489;fp;2;fpid;3)
6. [http://www.computerworld.com.au/index.php/id;405694618;  
fp;16;fpid;0](http://www.computerworld.com.au/index.php/id;405694618;fp;16;fpid;0)
7. [http://ddanchev.blogspot.com/2005/12/insiders-insights-  
trends-and-possible.html](http://ddanchev.blogspot.com/2005/12/insiders-insights-trends-and-possible.html)
8. [http://english.people.com.cn/200605/31/eng20060531\\_269  
908.html](http://english.people.com.cn/200605/31/eng20060531_269908.html)
9. <http://gaxed.com/>

345

## 2.6

### June

346

### **May's Security Streams (2006-06-03 12:29)**

Here's May's summary of all the security streams during the month. This is perhaps among the few posts in which I

can actually say something about the blog, the individual behind it, and its purpose, which is to - question, provoke,

and inform on the big picture. After all, "*I want to know God's thoughts... all the rest are details*", one of my favorite

[1]Albert Einstein's quotes. The way we often talk about a false feeling of security, we can easily talk about a false feeling of blogging, and false feeling of existence altogether. It is often assumed that the more you talk, the more you know, which is exactly the opposite, those that talk know nothing, those that don't, they do. There's nothing wrong with that of [2]referring to yourself, as enriching yourself through past experience helps you preserve your own unique existence, and go further. Awakening the full potential within a living entity is a milestone, while self preservation may limit the very development of a spirit - or too much [3]techno thrillers recently? :)

It's great to see that a knowledgeable audience has become a daily reality at this blog, it's never too late to meet new friends or their pseudo personalities. I've also included this month's stats area graph so you can get a grasp of the activity, go through past summaries for - [4]January, [5]February, [6]March and [7]April, in case your brain is hungry for more knowledge.

It is my opinion that the more uninformed the end user is, the less incentive for the vendors to innovate at the bottom line, and on the other hand, it is also easier for a vendor to put emphasize on current trends, instead of emerging ones - which is what is going to add value to its proposition in the long-term. **It's more profitable to treat**

**the disease, instead of curing it.** And while curing one doesn't mean curing all, it's a progress. So, I inform both sides and everyone in between. Information has never been free, but it wants to be free, so enjoy, [8]syndicate, and

keep yourself [9]up-to-date with my perception on information warfare and information security, even when I'm not

blogging, but just linking!

### **01. [10]Biased Privacy Violation**

While the site's niche segment has a lot of potential, I doubt it would scale enough to achieve its full effect. Providing Ex-couples with the microphone to express their attitudes is as quistionable as whether playing 3D shooters actually

limits or increases violence.

### **02. [11]Travel Without Moving - Typhoon Class Submarines**

There're a lot of strategic security issues going beyond the information security market, and that is the defense

and intelligence community's influence on the world. What used to be a restricted, or expensive practice, satellite

imageryis today's Google Earth/Maps's service on a mass scale, anyone can zoom in front of the NSA. And as it's

obvious you can spot things you can somehow define as sensitive locations though Google Earth/Maps, the question

is so what? I've managed to dig quite some interesting locations I haven't seen posted anywhere and will be adding

them shortly, feel free to suggest a spot if you have something in mind. The series in no way compete with the

[12]Eyeball-Series.org, though I wish.

### **03. [13]The Current State of Web Application Worms**

Web application worms, their potential and possible huge-scale impact is a topic that's rarely covered as an emerging trend by the mainstream media sources. On the other hand, over 200 words articles on yet another malware variant going in depth into how the Internet is driving force for the E-commerce revolution, and how a ransomware piece of malware is changing this. The problem is rather serious due to the common type of web application vulnerabilities huge eyeball aggregators suffer from. Whether it's speed or infected population to use as a benchmarking tool, just like packet-type of worms, web application worms are fundamental for the creation of a Superworm beneath the AV sensor's radar.

### **04. [14]Shaping the Market for Security Vulnerabilities Through Exploit Derivatives**

Resoucesful post providing overview of the most recent developments in the emerging market for software vulnera-

347

bilities, and the possibility to secure future vulnerability releases. As Adam at [15]Emergentchaos.com pointed out,

the legality of such markets is among the cons of the idea, which is perhaps the time to consider the usability of

markets for what's turning into a commodity - security vulnerabilities. The major problem which prompts for the

need of such, is the current "private club" only vulnerability sharing practices among the infomediaries, but it can easily be argued that empowering vulnerability diggers, not researchers, isn't the smartest thing the community can

do.

Vendors are often discussed as liable for the vulnerabilities in their software, but it's like blaming a dating ser-

vice for not generating you dates, my point is that you cannot simply blame vendors for the vulnerabilities in their

software as it would result in a major slowdown of innovation. Think about it, we all hate Bill Gates and use, while

trying to avoid Microsoft's products pretty much everywhere, monocultures are bad, we'd better have half the

Internet using MACs, and the other Windows so there would be an incentive and fair "allocation of resources"

targeting both sides, as the plain truth is that **malicious attackers aren't just attacking these days, they are gaining scale and becoming efficient**. In a free market, where market forces invisibly shape and guide it, there's little room for socially oriented initiatives like these. Today's software and technologies are shipped to get adapted, that's

insecure ones we become dependent on, to later find out we have the live with their insecurities – no one is perfect,

and being all well-rounded is so boring at the bottom line.

If we were to start "thinking Security" everywhere, there wouldn't be anything left in respect to usability at the end of the day. And as I've pointed out in a previous post on [16]valuing security, if security doesn't bring

anything tangible, but prevents risks, that's the cornerstone of the problems arising with justifying expenditures.

The Internet we've become so addicted and dependent on wasn't build with security in mind, but our conscious

or subconscious marginal thinking gave us no choice, either live with the vulnerabilities and take advantage of its

benefits, or stop using it at all. If we were to start thinking security first, there wouldn't be Internet at all, at least not in our lifetime. ISPs avoiding to take action on customers participating in botnets as they still haven't managed to find a way to commercialize the service, or Microsoft shipping its products in root mode and with all features turned on

by default, are important points to keep in mind when refering to the practice of threatening and not curing deceases.

You cannot blame vendors for the security vulnerabilities in their software, you can blame them for the huge

windows of opportunities their lack of action opens, and lack of overall commitment towards mitigating the threats



posed by these, now, how you would you go to turn your day dreaming into a measurable metric, even come up with

a benchmark is challenging – a challenge ruined by the value of keeping an 0day, a truly 0day one.

#### **05. [17]The Cell-phone Industry and Privacy Advocates VS Cell Phone Tracking**

There you go with your fully realistic 1984 scenario, I wonder would the idea constitute mass surveillance and

social networking analysis altogether. DIY alternatives are gaining popularity, and the cell phone industry doesn't

really want to be perceived as an "exact location"provider, rather communication services. The excuse if it becomes habitual? Well, since there's no Cold War anymore – just sentiments – it's Terrorism today.

#### **06. [18]Snooping on Historical Click Streams**

It was about time Google reposition itself as a search company, not as a new media one heading towards portalization.

There's nothing wrong with the idea, the reality is they can never catch up with Yahoo – and they shouldn't! Spending

some time with the feature, and you will be able to verify most of your previous research findings, or come across to

surprising ones. Do you trust Google and its geolocation services at the bottom line? I do.

#### **07. [19]Pass the Scissors**

It's never too late to earn a buck for printing currency, even in times of inflation in between.

#### **08. [20]Is Bin Laden Lacking a Point?**

Google trends point to Washington DC as the region with the highest interest in [21]Bin Laden, not surprising isn't it?

348

I feel the entire idea of an organizational hierarchy and Bin Laden on the top is an outdated thinking, but a marketable one forwarding the entire responsibility to one person, who at the end of day wouldn't have any choice but to

accept it, even though he had nothing to do with something in particular. Leadership is critical, and so is possible

successorship. An image is worth a thousand words in this case!

#### **09. [22]Pocket Anonymity**

Harnessing the power of established brands in privacy, encryption and anonymity services and providing portability is

a great idea, no doubt, but what I'm missing is a targeted market, a clear positioning, is it [23]privacy or anonymity

provider, as there's a huge difference between the two of these. A free alternative to the idea as well.

#### **10. [24]Travel Without Moving - Scratching the Floor**

No comment, just awareness.

#### **11. [25]Terrorist Social Network Analysis**

Seems like social network analysis practices apply to terrorist organizations as well, and why wouldn't they? As you

can see, there isn't big of a different between a Fortune 500 organization, and a terrorist one, the only problem and

downsize is the inability to take advantage of the momentum, historical findings out of data mining are useful for

power point slides seeking further investment, and that's it.

## **12. [26]Valuing Security and Prioritizing Your Expenditures**

Reactive, Proactive, or Adaptive, what's your security strategy, and what's your return on security investment?

## **13. [27]EMP Attacks - Electronic Domination in Reverse**

Did you know that Stalin was aware of the U.S's A-bomb, even before Harry Truman was? – the consequence of too

much secrecy sometimes! EMP attacks get rarely discussed, yet today's portability of these and potential for chaos

put them on the top of my watch list. There have been numerous ongoing Cybersecurity and critical infrastructure

security exercises in the U.S for the last couple of years, and while military equipment goes through hardening process,

Russia remains a key innovator whose capabilities have surpassed their own expectations. Cyber warfare is the next

Revolution in Military Affairs, and it would be naive not to keep thinking of sneaky attacks, the weakest point in an IT

and electronics dependent society.

#### **14. [28]Insider Competition in the Defense Industry**

Where else, if not in the defense industry?

#### **15. [29]Techno Imperialism and the Effect of Cyberterrorism**

Today's public perception of Cyberterrorism is so stereotyped, perhaps due to one basic reality - you cannot fight

Cyberterrorism, the way you can blow up a cave in Afghanistan, and it's a big problem. While public accountability is

easily achieved through Cybersecurity exercises, there isn't a better tool for propaganda, recruitment, communica-

tion and research than the Internet, and as you're about to find out, there are ongoing initiatives to crawl the Web

for terrorist web sites, analyze terrorist speaking communication patterns on web forums, and how encryption, flight

simulator programs are an unseperable reality of the concept.

As the conspiracy theorist inside me is screaming, there used to be a speculation how Disney on purposely

brainwashed the perception of UFOs in its content, to make it more user-friendly excuse, and put everyone who's

talking the opposite turns into the usual " *that's the guy that has seen them*" unfavorable position. Today's coverage

on Cyberterrorism doesn't provoke discussion, instead it always tries to communicate and question the credibility of the idea, with the usual scenarios relating to SCADA devices, terrorists melting down power plants and the rest of the science-fiction stories. In all my posts on Cyberterrorism, a topic I've been actively writing on, and following for some years, I always point out that terrorists are not rocket scientists unless we make them feel so - or have benefits to think they are.

349

#### **16.** [30]Travel Without Moving - Cheyenne Mountain Operations Center

Cheyenne Mountain Operations Center from Google Maps, and a summary of a report on Google Earth's security

implications, I hope you'll manage to get your hands on, the way I did through a friend.

#### **17.** [31]Nation Wide Google Hacking Initiative

I like the idea of auditing a nation's cyber space through Google Hacking, the only problem is communicating the

value to public and to the companies/sites. What can be defined as sensitive information leaked through Google,

and who's the attacker? Is it a script kiddie, a google hacker, a foreign intelligence personel, or foreign company

conducting unethical competitive intelligence? Knowing, or at least theorizing on the possible adversaries will lead

your auditing practices to an entirely new level.

**18. [32]Espionage Ghosts Busters**

No government is comfortable with having to smile at Chinese people, or how their economy is evolving from

supplier to manufacturer, still there isn't any serious ground for this case – besides and uncomfortability issue.

**19. [33]Arabic Extremist Group Forum Messages' Characteristics**

Great research on today's fully realistic scenario of terrorists communicating over the Web, the public one, as basic

authentication would have stopped such automated approaches for sure. What can you actually find with that

type of intelligence, real terrorists communications, or growing propaganda sentiments, in between pro-democratic

individuals to be recruited?

**20. [34]The Current, Emerging, and Future State of Hacktivism**

A very well researched dissertation, a lot of visionary thoughts while it goes back to the basics. It is doubtful whether hacktivism would cease to exist despite the for-profit malicious attacks these days, as anarchists, governments,

patriots or script kiddies, they all have an opinion on how things should be.

**21. [35]Bedtime Reading - The Baby Business**

What's a "better" kid, and why you don't need one?  
Controllable uncertainty can be exciting sometimes, but as always, life's too short to live with uncertainty!

## **22. [36]Travel Without Moving - Korean Demilitarized Zone**

A post with an emphasis on North Korea, which as a matter of fact got recently [37]a decline from the U.S on two-way

talks on whether the U.S would condemn their nuclear program. As I've pointed out, there are just looking for

attention, while the U.S is sticking to six way talks only. Iran truly took advantage of the overly bad publicity for the U.S around the world.

## **23. [38]Aha, a Backdoor!**

A smart way to fuel growth in homeland security solutions is to be able to exempt publicly traded companies from re-

porting these activities, and with the SEC trying to achieve better transparency in its data reporting practices, it opens up a huge backdoor for enterprises to take advantage of, without any short-term accountability, or transparency

requirements for the use of their stockholder's money. It's the corporate world!

## **24. [39]Forgotten Security**

Forgotten what if security plans on a possible assassination to be precise. It's a like a situation where a newly

graduated wannabe marketer is asked to conduct a marketing research for a future release of a product, and he just

opens his bag and brings out a textbook, and starts looking it up.

## **25. [40]Delaying Yesterday's "0day" Security Vulnerability**

Nothing groundbreaking as this is today's reality for everyone, and there isn't such thing as a true 0day vulnerability

350

these days. Oday to who, to the media, to the underground, to the market, or to the researcher who's catching up with a week of backlog?

## **26. [41]Who's Who in Cyber Warfare?**

In the future the majority of Cyber wars would be waged by nations, and the maturity of their understanding of the

concept, and actual capabilities is again going to put the masses as a hostage in between. Defensive or offensive

motives behind further development, armies will be defeated, and battles will be won in Cyberspace – whether by

infowar guerilla-fighters, corporations, or nations is the beauty of this uncertain growing reality.

## **27. [42]No Anti Virus Software, No E-banking For You**

Great idea, lot's of revenues for the AV vendor, end users with a feeling of security, all looks and sounds great, but it isn't, as these are the basics. An AV solution doesn't mean you won't get hacked, your financial information stolen,



and your home PC won't end up in a botnet, it means there's less chance for it to happen now. Is this campaign

worth the publicity and in respect to retaining the bank's customers? I feel it is, but it's where the whole process of bank2customer safety practices communication begins.

## **28. [43]Microsoft in the Information Security Market**

McAfee and Symantec have greatly felt the pressure from Microsoft's ambitions, as they've simultaneously released

information on their alternatives of OneCare, all-in-one security and PC tuning for the masses. Moreover, IP

violation suits and the rest truly represent the threat, and while I don't see any, I avoid the fact that this is what

the end user really needs. And with all the buzz about OneCare, Microsoft's distribution channels, channel partners

and strategic partnerships, it would be hard for them to stop using OneCare in an year. That's why McAfee, and

Symantec's releases of alternatives neatly ruined the pionner position Microsoft could have taken. Now it's the

same old information security market, the one you're so comfortable with, McAfee and Symantec providing security

solutions as their first priority, and Microsoft, positioned as a follower catching up. Smart move!

## **29. [44]Covert Competitive Intelligence**

With enterprises considering key extranet participants as potential attack vectors, and web-integration of backend

systems as potential targets, insiders are benefiting from within.

Dealing with "hackers", malware, firewalls

configuration etc. is part of the problem of perimeter based and application based defense. Consider taking into

consideration, organizational threats such as insiders, and figure out a cost-effective way of dealing with this hard to detect, measure and secure against threat.

### **30. [45]The Global Security Challenge - Bring Your Know-How**

How would you be more creative, knowing how much is your budget and trying to allocate it for the idea of allocating

it, or coming up with the idea first and then trying to commercialize it? Budget allocation is a daily practice, but the way it empowers, the very same way it wastes resources, ones usually wrongly allocated.

[46]Healthy Paranoia

I really feel you.

1.

<http://www.brainyquote.com/quotes/quotes/a/alberteins148836.html>

2. <http://mind.sourceforge.net/ego.html>

3. <http://cyberpunkreview.com/>

4. <http://ddanchev.blogspot.com/2006/01/januarys-security-streams.html>

5. <http://ddanchev.blogspot.com/2006/03/februarys-security-streams.html>
  6. <http://ddanchev.blogspot.com/2006/03/marchs-security-streams.html>
  7. <http://ddanchev.blogspot.com/2006/05/aprils-security-streams.html>
  8. <http://feeds.feedburner.com/DanchoDanchevOnSecurityAndNewMedia>
  9. <http://del.icio.us/ddanchev?settagview=cloud>
- 351
10. [http://ddanchev.blogspot.com/2006/05/biased-privacy-violation\\_03.html](http://ddanchev.blogspot.com/2006/05/biased-privacy-violation_03.html)
  11. <http://ddanchev.blogspot.com/2006/05/travel-without-moving-typhoon-class.html>
  12. <http://www.eyeball-series.org/>
  13. <http://ddanchev.blogspot.com/2006/05/current-state-of-web-application-worms.html>
  14. <http://ddanchev.blogspot.com/2006/05/shaping-market-for-security.html>
  15. [http://www.emergentchaos.com/archives/2006/05/economics\\_of\\_vulnerabilit.html](http://www.emergentchaos.com/archives/2006/05/economics_of_vulnerabilit.html)
  16. <http://ddanchev.blogspot.com/2006/05/valuing-security-and-prioritizing-your.html>

17. <http://ddanchev.blogspot.com/2006/05/cell-phone-industry-and-privacy.html>
18. <http://ddanchev.blogspot.com/2006/05/wiretapping-voip-order-questioned.html>
19. <http://ddanchev.blogspot.com/2006/05/pass-scissors.html>
20. <http://ddanchev.blogspot.com/2006/05/is-bin-laden-lacking-point.html>
21. <http://www.google.com/trends?q=Bin+Laden>
22. <http://ddanchev.blogspot.com/2006/05/pocket-anonymity.html>
23. <http://ddanchev.blogspot.com/2006/01/anonymity-or-privacy-on-internet.html>
24. <http://ddanchev.blogspot.com/2006/05/travel-without-moving-scratching-floor.html>
25. <http://ddanchev.blogspot.com/2006/05/terrorist-social-network-analysis.html>
26. <http://ddanchev.blogspot.com/2006/05/valuing-security-and-prioritizing-your.html>
27. <http://ddanchev.blogspot.com/2006/05/emp-attacks-electronic-domination-in.html>
28. <http://ddanchev.blogspot.com/2006/05/insider-competition-in-defense.html>
29. <http://ddanchev.blogspot.com/2006/05/techno-imperialism-and-effect-of.html>

30. <http://ddanchev.blogspot.com/2006/05/travel-without-moving-cheyenne.html>
31. <http://ddanchev.blogspot.com/2006/05/nation-wide-google-hacking-initiative.html>
32. <http://ddanchev.blogspot.com/2006/05/espionage-ghosts-busters.html>
33. <http://ddanchev.blogspot.com/2006/05/arabic-extremist-group-forum-messages.html>
34. <http://ddanchev.blogspot.com/2006/05/current-emerging-and-future-state-of.html>
35. <http://ddanchev.blogspot.com/2006/05/bedtime-reading-baby-business.html>
36. [http://ddanchev.blogspot.com/2006/05/travel-without-moving-korean\\_27.html](http://ddanchev.blogspot.com/2006/05/travel-without-moving-korean_27.html)
37. [http://abcasiapacific.com/news/stories/asiapacific\\_stories\\_1653722.htm](http://abcasiapacific.com/news/stories/asiapacific_stories_1653722.htm)
38. <http://ddanchev.blogspot.com/2006/05/aha-backdoor.html>
39. <http://ddanchev.blogspot.com/2006/05/forgotten-security.html>
40. <http://ddanchev.blogspot.com/2006/05/delaying-yesterdays-0day-security.html>
41. <http://ddanchev.blogspot.com/2006/05/whos-who-in-cyber-warfare.html>

- 42. <http://ddanchev.blogspot.com/2006/05/no-anti-virus-software-no-e-banking.html>
- 43. <http://ddanchev.blogspot.com/2006/05/microsoft-in-information-security.html>
- 44. <http://ddanchev.blogspot.com/2006/05/covert-competitive-intelligence.html>
- 45. <http://ddanchev.blogspot.com/2006/05/global-security-challenge-bring-your.html>
- 46. <http://ddanchev.blogspot.com/2006/05/healthy-paranoia.html>

352

### **Travel Without Moving - KGB Lubyanka Headquarters (2006-06-04 17:26)**

Yet another [1]hot spot in this week's [2]Travel Without Moving series - this time it's [3]Lubyanka Square's KGB

Headquarters. There are still lots of Cold War sentiments in the air among yesterday's and today's super powers

and you just can't deny it. [4]Today's [5]FSB, the successor to the [6]KGB, is taking a very serious approach towards

[7]counter-intelligence, and [8]offensive scientific intelligence practices in a much more synergetic relationship with

the academic world compared to years ago. While the CIA is undisputably the most popular foreign intelligence

agency, and more of a front end to the NSA itself from my point of view, the KGB still remains responsible for very

important and "silent" moments in the world's history. There were moments in the very maturity of the Cold War, when both, the CIA, and the KGB were on purposely disinforming their operatives in order to keep them motivated

and fuel the tensions even more, but compared to the CIA with its technological know-how, [9]KGB's HUMINT

capabilities didn't get surpassed by technologies. Among the key success factors for the intelligence agency was

the centralized nature of the command of chain, total empowerment, common and obsessive goal, and clear enemy.

Today's trends mostly orbit around :

- information sharing, that is less complexity among different departments and agencies
- win-win information sharing among nations
- offensive and defensive CYBERINT, harnessing the power, or protecting against the threats posed by the digital era
- automated and efficient mass surveillance practices-eliminating "safe heavens"

In case you really want to go in-depth into what has happened during the last couple of decades, [10]Vasilli

Mitrohih's KGB Archives are worth reading. And the true-retro gamers can take the role of " *Captain Maksim*

*Mikhailovich Rukov, recently transferred to the Department P from the GRU after three years' duty to investigate*

*possible corruption inside the KGB (after a former agent turned private eye was found murdered). However, as the*

*plot progresses, Rukov finds himself investigating a party hardliner anti-perestroika plot that threatens the life of General Secretary Mikhail Gorbachev" while [11]playing [12]KGB - Conspiracy game.*

1. <http://maps.google.com/maps?t=k&hl=en&ll=55.759875,37.627155&spn=0.005385,0.014162&om=1>
2. <http://ddanchev.blogspot.com/2006/05/travel-without-moving-cheyenne.html>
3. <http://www.fas.org/irp/world/russia/kgb/lubyanka.htm>
4. [http://en.wikipedia.org/wiki/Federalnaya\\_Sluzhba\\_Bezopasnosti](http://en.wikipedia.org/wiki/Federalnaya_Sluzhba_Bezopasnosti)
5. <http://www.fsb.ru/>
6. <http://en.wikipedia.org/wiki/KGB>
7. <http://ddanchev.blogspot.com/2006/02/top-level-espionage-case-in-greece.html>
8. <http://en.wikipedia.org/wiki/FAPSI>
9. <http://fas.org/irp/world/russia/program/humint.htm>
10. <http://www.amazon.com/gp/product/0465003109/002-1508184-6724032?v=glance&n=283155>
11. [http://www.abandonia.com/games/93/KGB\(akaConspiracy\).](http://www.abandonia.com/games/93/KGB(akaConspiracy))



12. [http://en.wikipedia.org/wiki/KGB\\_\(computer\\_game\)](http://en.wikipedia.org/wiki/KGB_(computer_game)).

353

### **Skype as the Attack Vector (2006-06-04 17:52)**

It's often hard to actually measure the risk exposure to a threat, given how overhyped certain market seg-

ments/products' insecurities get with the time. Gartner, and the rest of the popular marketing research agencies

seem to be obsessed with [1]Skype as the major threat to enterprises, while Skype [2]isn't really bad news, [3]com-

pliance is, in respect to [4]VoIP, P2P, IM and Email communications retention or monitoring. From the [5]article :

*" The most recent bug in Skype is another clue to enterprises that they should steer clear of the VoIP service, research firm Gartner recently warned. Two weeks ago, Skype patched a critical vulnerability that could let an*

*attacker send a file to another user without his or her consent, and potentially obtain access to the recipient's*

*computer and data. This vulnerability follows three in 2005 (two high-risk, one low-risk) and highlights the risk of not establishing and implementing an enterprise policy for Skype," wrote Gartner research director Lawrence Orans in an online research note. "Because the Skype client is a free download, most businesses have no idea how many Skype clients are installed on their systems or how much Skype traffic passes over their networks. "*

There's a slight chance an enterprise isn't already blocking Skype, using both, [6]commercial and [7]public

methods wherever applicable. Moreover, it would be much more feasible to consider the fact that, if the enterprise

- assuming a U.S one - isn't blocking the use of Skype, it must somehow monitor/retain its use in order to comply

with [8]standard regulations. Skype poses the following problems :

- inability for the enterprise to retain the IM and VoIP sessions in accordance with regulations

- wasted bandwidth costing loss productivity and direct cash outflows, slowdown for critical network functions

- covert channels possibilities

Several months ago, Skype was also discussed as a [9]command'n'control application for botnets, while [10]steganog-

raphy based communications and [11]plain-simple encrypted/stripped IRCd sessions remain rather popular. Malware

authors are actively looking for ways to [12]avoid IRC given the [13]popularity it has gained and the experience

[14]botnet hunters have these days.

Skype is the last problem to worry about, as in this very same way the recent [15]vulnerabilities in major mar-

ket leading AVs would have had a higher risk exposure factor as there's a greater chance of occurrence of malware,

than a Skype vulnerability. It's the vulnerabilities in software in principle you have to learn how to deal with, and

third-party applications that somehow make it on your company's network.

More resources :

[16]Skype Security Evaluation

[17]Silver Needle in the Skype

[18]Skype Security and Privacy Concerns

[19]Impact of Skype on Telecom Service Providers

1. <http://news.google.com/news?hl=en&ned=us&q=skype%2Bsecurity>
2. [http://www.gartner.com/resources/140900/140991/act\\_now\\_to\\_combat\\_the\\_growin\\_140991.pdf](http://www.gartner.com/resources/140900/140991/act_now_to_combat_the_growin_140991.pdf)
3. <http://http://www.bluecoat.com/solutions/security/compliance.html>
4. <http://ddanchev.blogspot.com/2006/05/wiretapping-voip-order-questioned.html>
5. <http://www.itnews.com.au/newsstory.aspx?ClaNID=33194>
6. [http://www.bluecoat.com/downloads/whitepapers/BCS\\_controlling\\_skype\\_wp.pdf](http://www.bluecoat.com/downloads/whitepapers/BCS_controlling_skype_wp.pdf)
7. [http://www.net-security.org/dl/articles/Blocking\\_Skype.pdf](http://www.net-security.org/dl/articles/Blocking_Skype.pdf)

8. <http://www.windowsecurity.com/articles/How-Do-Compliance-Issues-Affect-your-Network.html>
9. <http://ddanchev.blogspot.com/2006/01/skype-to-control-botnets.html>
10. <http://digiassn.blogspot.com/2006/03/securityc-demonstration-of.html>

354

11. <http://ddanchev.blogspot.com/2006/02/master-of-infected-puppets.html>
12. <http://www.enre.umd.edu/content/rmeyer-assessing.pdf>
13. <http://www.symantec.com/avcenter/reference/the.evolution.of.malicious.irc.bots.pdf>
14. <http://www.shadowserver.org/>
15. <http://www.internetnews.com/security/article.php/3609846>
16. <http://www.skype.com/security/files/2005-031%20security%20evaluation.pdf>
17. [http://www.secdev.org/conf/skype\\_BHEU06.pdf](http://www.secdev.org/conf/skype_BHEU06.pdf)
18. <http://www.securityfocus.com/columnists/357>
19. [http://www.commnw.com/reports/EVS-Impact\\_of\\_Skype\\_on\\_Tele\\_Opr-January10.pdf](http://www.commnw.com/reports/EVS-Impact_of_Skype_on_Tele_Opr-January10.pdf)

355

**Where's my Fingerprint, Dude? (2006-06-06 19:25)**

[1]Personal data security breaches [2]continue occurring, and with the trend towards evolving to a digital economy,

it's inevitably going to get ever worse. In a recently revealed case "[3]Lost IRS laptop stored employee fingerprints", from the article :

*" A laptop computer containing fingerprints of Internal Revenue Service employees is missing, MSNBC.com has*

*learned. The computer was lost during transit on an airline flight in the western United States, IRS spokesman Terry Lemon said. No taxpayer information was on the lost laptop, Lemon said. In all, the IRS believes the computer*

*contained information on 291 employees and job applicants, including fingerprints, names, Social Security numbers,*

*and dates of birth. "*

For the time being the largest accommodator of fingerprints in the world is the U.S.A, and this fact affects

anyone that enters the U.S. My point is that, given the unregulated ways of classifying, storing, transferring and

processing such type of information would result in its inevitable loss – bad in-transfer security practices or plain

simple negligence.

As we're also heading to a biometrics driven society, the impact of future data security breaches will go way

beyond identity theft the way we know it – lost and stolen voice patterns, DNAs, and iris snapshots would make

the headlines. You might also be interested in knowing how close that type of "future scenario" really is given the

[4]modest genetic database of 3 million Americans already in existence.

Things are going to get very ugly, and it's not the privacy issue that bothers me, but the aggregation of such

type of data at the first place, and who will get to steal it. It's perhaps the perfect market timing moment to start a

[5]portable security solution provider, or resell ones know-how under license, of course.

1. <http://ddanchev.blogspot.com/2006/01/personal-data-security-breaches.html>

2. <http://news.google.com/news?hl=en&ned=us&q=data%2Bbreach&ie=UTF-8>

3. <http://www.msnbc.msn.com/id/13152636/>

4. <http://www.washingtonpost.com/wp-dyn/content/article/2006/06/02/AR2006060201648.html>

5. [http://www.csoononline.com/read/050106/portable\\_data.html](http://www.csoononline.com/read/050106/portable_data.html)

356

### **Phantom Planes in the Skies (2006-06-06 19:37)**

I can barely imagine the panic with a non-responding – can it respond when it's not there? – plane in the sky, at least

by the time a visual confirmation reveals the truth. In the post 9/11 world, airports were among the first strategic

targets to get the funding necessary to protect against the threats fabricated in a think-tank somewhere. Money are

wasted in this very same fashion on a daily basis, with no clear ROI, just established social responsibility and common

sense security. Disinformation can always happen in sky, as "[1]Flaw may lead to air chaos". From the article :

*" Hackers armed with little more than a laptop could conjure up phantom planes on the screens of Australia's*

*air traffic controllers using new radar technology, warns Dick Smith. The prominent businessman and aviator claims*

*to have found another serious security flaw in the new software being introduced into the air traffic control system.*

*He has challenged Transport Minister Warren Truss to allow him to set up a demonstration of the problem at a test of the technology in Queensland to show how hackers could exploit the automatic dependent surveillance broadcasting*

*(ASD-B) system to create false readings on an air traffic controller's screen. The air space activist says he was told of the flaw by US Federal Aviation Administration staff. "*

Compared to a speculation I described in a previous post "[2]Why's that radar screen not blinking over there?", these practices are highly natural to [3]ELINT planes/warfare, and in the capabilities of experienced staff members

as pointed out in the article. Everything is buggy, and so is the [4]ASD-B system for sure, but the problem from my

point of view, is the possibility for a "[5]talkative leakage", and the procedures, if any, to internally report bugs like

these, and get them fixed of course.

Phantom Warhawk image courtesy of Les Patterson.

1. <http://australianit.news.com.au/articles/0,7204,19375464%5E15331%5E%5Enbv%5E15306%2D15318,00.html>
2. <http://ddanchev.blogspot.com/2006/04/whys-that-radar-screen-not-blinking.html>
3. <http://en.wikipedia.org/wiki/ELINT>
4. [http://en.wikipedia.org/wiki/Automatic\\_Dependent\\_Surveillance-Broadcast](http://en.wikipedia.org/wiki/Automatic_Dependent_Surveillance-Broadcast)
5. <http://ddanchev.blogspot.com/2005/12/insiders-insights-trends-and-possible.html>

357

### **Bedtime Reading - Rome Inc. (2006-06-08 17:21)**

If the [1]Baby Business helped you envision the future, "[2]Rome Inc - The Rise and Fall of the First Multinational Corporation" is going to help you perceive the past within today's corporate culture - and [3]Stanley Bing makes good points on every stage of the empire.

Basically, the book emphasizes on the "first multinational corporation" Rome, selling the ultimate product of

its time - citizenship. Moreover, it goes in-depth into the concept of moguls and anti-moguls, and how their tensions



indeed create an entrepreneurial and corporate culture in 120 A.D.

Every industry has moguls and anti-moguls, the behind the curtain disruptors at a specific stage. What are

some of the characteristics of a mogul?

- Commission their PR
- Exercise power when feeling endangered – elephants against the mice warfare
- Indirectly control the media that's "winning points" for quotations, and "credible" content
- Generally, tend to believe in being the Sun, when the universe tends to have so many dwarfs, and dimensions altogether
- Hide behind C-level positions
- Talk more than actually listen
- When they sneeze the whole industry gets cold

Certain societies, if not all, get obsessed with superficially creating heroes, so professionally that at a certain

point, the "hero" cannot deny any of the praises, but starts living with them and the load that comes altogether. Get hold of this masterpiece, you're gonna love it!

1. <http://ddanchev.blogspot.com/2006/05/bedtime-reading-baby-business.html>

2. <http://www.amazon.com/gp/product/0393060268/002-5173094-2416853?v=glance&n=283155>

3. <http://stanleybing.com/>

358

### **An Over-performing Spammer (2006-06-08 17:32)**

The frequency of sending spam messages is evolving like never before, and while spammers are still catching up with the newest technologies such as [1]VoIP, [2]WiFi, Cell phones – newest at least in respect to spamming – trying to avoid the now mature industry's practices, and taking advantage of the growing economies and their newbie users as victims, is what keeps it going.

I simply couldn't resist not to share this, seems like this spammer is totally overperforming himself.

How

would I fell a victim into this, given I cannot read what I'm about to get scammed with?

Spammers today are in a world of pain when it comes to the industry's experience in detecting their mes-

sages, still, spam continues to represent the majority of email traffic worldwide, and it's getting more creative.

Images, "marketing" messages that you can barely read, old psychological tricks, but still, out of couple of million messages, someone still takes it personal, and feels like making a deal online.

Why spamming works? Because of the ubiquity of email, because of the freely available, marketed as fresh, email lists, and at the bottom line, the price for a spammer to send couple of million emails is getting lower with botnets on demand becoming a commodity. End users, end up sending spam to themselves for being infected with malware. What's next? Spamming is still catching up with the technological possibilities, and Chinese telecom operators for instance happen to be the most experienced ones in filtering [3]mobile phones spam – guess they're also over-performing in between [4]censorship.

1. [http://en.wikipedia.org/wiki/Spit\\_\(VoIP\\_spam\)](http://en.wikipedia.org/wiki/Spit_(VoIP_spam)).
2. <http://www.vnunet.com/vnunet/news/2122838/spammers-target-wi-security>.
3. [http://en.wikipedia.org/wiki/Mobile\\_phone\\_spam](http://en.wikipedia.org/wiki/Mobile_phone_spam)
4. <http://ddanchev.blogspot.com/2006/02/chinese-internet-censorship-efforts.html>

359

### **Brace Yourself - AOL to Enter Security Business (2006-06-09 15:49)**

In the re-emergence of the Web, AOL got the attention it never imagined it would get, [1]Microsoft and Google

fighting for a share of its modest, but strategic amount of eyeballs. After being an exclusive part of Time Warner's

balance sheet since its early acquisition, and with a [2]  
\$510M fine, dial-up business that was profitable by the time  
telecoms started offering cable connections, due to the  
years of infrastructure renovation, the thought to be mature  
online advertising model is what saved it. Now, AOL is  
basically putting half its leg into the red hot [3]security  
market and wisely playing it safe as :

*" AOL plans to expand into security services with the release  
of the Active Security Monitor, expected on Thursday. The  
program would also check to make sure Internet Explorer is  
properly configured to prevent security holes.*

*"ASM determines a security score for your PC, and for all  
other PCs in your home network, by evaluating the status of  
all the major components needed for a robust system: Anti-  
Virus software, Anti-Spyware software, Firewall*

*protection, Wireless Security, Operating System, Web  
Browser, Back up software and PC Optimization. "*

After the scoring, I presume it would "phone back home" and  
let AOL know what end users are mostly miss-

ing, then a solution provided by AOL, or a licensee would  
follow. Benchmarking against AOL's understanding of

application based security is tricky, and I bet you already  
know the programs necessary to establish common sense

security on your PC/network. Who's next to enter the  
security industry besides [4]Microsoft and AOL, perhaps

DoubleClick?

CNET has naturally [5]reviewed the Active Security Monitor.

1.

[http://www.nytimes.com/2005/12/19/business/media/19aol.html?  
ex=1292648400&en=98f969353457b3a4&ei=5088&partn  
er=rssnyt&emc=rss](http://www.nytimes.com/2005/12/19/business/media/19aol.html?ex=1292648400&en=98f969353457b3a4&ei=5088&partner=rssnyt&emc=rss)

2.

[http://www.bizjournals.com/washington/stories/2004/12/13/  
daily16.html](http://www.bizjournals.com/washington/stories/2004/12/13/daily16.html)

3.

[http://www.betanews.com/article/AOL\\_to\\_Enter\\_Security\\_Bu  
siness/1149718558](http://www.betanews.com/article/AOL_to_Enter_Security_Business/1149718558)

4. [http://ddanchev.blogspot.com/2006/05/microsoft-in-  
information-security.html](http://ddanchev.blogspot.com/2006/05/microsoft-in-information-security.html)

5.

[http://reviews.cnet.com/AOL\\_Active\\_Security\\_Monitor/4505-  
3667\\_7-31929463.html?tag=subnav](http://reviews.cnet.com/AOL_Active_Security_Monitor/4505-3667_7-31929463.html?tag=subnav)

360

### **Unknowingly Becoming a Child Porn King (2006-06-10 16:26)**

The old dilemma, is the user blaming malware on purposely, or what I'm not surprised is that it actually happened –

[1]hacker being the colleague next desk, or the user himself, in this case for instance.

*" An Amanzimtoti man accused of possessing thousands of computerised child pornography images is expected*

*to raise a technical defence - that he was a victim of a hacker who downloaded the images on to his computer without his knowledge. At least six people had access to his computer at any given time and there was no password. "*

While I've [2]mentioned on the possibilities of "Anonymous and illegal hosting of (copyrighted) materials" in

*the future as " Picture a huge distributed storage capability, where the loss of a single host, wouldn't affect the actual dissemination of the files in question, neither it would influence the rise of bandwidth usage. BitTorrent*

*disrupted the concept of transferring huge files over the Net. As we've already witnessed during December, 2005, a*

*relatively modest, still powerful enough [3]botnet of 18, 000 computers started using BitTorrent to transfer pirated files over the hosts. Certain users will definitely wake up as true porn kings :)" I don't think that's the case here though.*

Find a list of international organizations on [4]how to report child pornography.

1. [http://www.iol.co.za/index.php?set\\_id=1&click\\_id=15&art\\_id=vn20060609051241794C647148](http://www.iol.co.za/index.php?set_id=1&click_id=15&art_id=vn20060609051241794C647148)

2. <http://www.linuxsecurity.com/docs/malware-trends.pdf>

3. <http://www.eweek.com/article2/0,1759,1904429,00.asp?kc=EWRSS03119TX1K0000594>

4. [http://www.tinhat.com/children/report\\_pornography.html](http://www.tinhat.com/children/report_pornography.html)

## **All Your Confidentiality Are Belong To Us (2006-06-10 16:49)**

The proof that commercial and open source [1]encryption has surpassed the technologies to police it, or the idea

that privacy and business growth as top priorities would ruin the whole initiative?

*" The Government has launched a public consultation into a draft code of practice for a controversial UK law*

*that critics have said could alienate big business and IT professionals. Part III of the Regulation of Investigatory Powers Act 2000 (RIPA) will, as it stands, give police the authority to force organisations and individuals to disclose encryption keys. The Government issued the public consultation on the code of practice for Part III, which will regulate how police and the courts use powers under the legislation, on Wednesday. "*

It would be interesting to see how they would initiate the response from individuals, without raising the the

eyebrows on the majority of civil liberties watch dogs out there and, of course, businessess. That's of course, assum-

ing they use encryption at the first place. Could be much more "wiser" to take advantage of covert practices to obtain the necessary information, instead of "forcing" this measure – detecting encrypted/covert communication channels is another topic. Moreover, compared to the Australian [2]police whose capabilities of obtaining information on

criminals include the use of spyware is a bit contraversial, but adaptave approach.

If national infrastructure security matters, have individuals and enterprises personally take care of their secu-

urity and encryption keys, promote data encryption, instead of dictating the vibrations by slowing down the basics

through such laws.

1.

<http://news.zdnet.co.uk/internet/security/0,39020375,39273873,00.htm>

2. [http://news.com.com/Australian+police+get+go-ahead+on+spyware/2100-7348\\_3-5491671.html](http://news.com.com/Australian+police+get+go-ahead+on+spyware/2100-7348_3-5491671.html)

362

### **There You Go With Your Financial Performance Transparency (2006-06-10 16:57)**

Truly amazing, and the inevitable consequence of communication retention in the financial sector, but I feel it's the

[1]magnitude that resulted in [2]Enron's entire email communication archive that's seems available online right now.

"[3] *Search through more hundreds of thousands of email messages to and from 176 former* [4] *Enron execu-*

*tives and employees from the power-trading operations in 2000-2002. For the first time, they are available to the*

*public for free through the easy-to-use interface of the* [5] *InBoxer Anti-Risk Appliance.* [6] *Create a free account, and*



*go to work. You can search for words, phrases, senders, recipients, and more. "*

The interesting part is how their [7]ex-risk management provider is providing the data, in between fighting

with the [8]Monsters in Your Mailbox.

1. <http://en.wikipedia.org/wiki/Enron>
2. <http://www.enronemail.com/>
3. <http://media.inboxer.com/antiriskgwy.html>
4. <http://news.bbc.co.uk/1/hi/business/1780075.stm>
5. <http://www.inboxer.com/>
6. <http://media.inboxer.com/antiriskgwy.html>
7. <http://www.inboxer.com/>
8. [http://www.inboxer.com/downloads/Monsters\\_In\\_Your\\_Mailbox.pdf](http://www.inboxer.com/downloads/Monsters_In_Your_Mailbox.pdf)

363

### **Going Deeper Underground (2006-06-10 17:11)**

IT Security Goes Nuclear, at least [1]that's what they say.

*" Venture capitalists are predicting a "business boom below ground" as blue-chip companies turn to nuclear bunkers built at the height of the Cold War in the battle to protect sensitive electronic data. The latest private equity investor to move in on the area is Foresight Venture Partners, which*

*has just taken a 20 per cent stake in The Bunker Secure Hosting. "*

But no matter how [2]deep underground you are, you would still be providing an Internet connection given

you're a hosting company. That's an open network, compared to a closed one which is more easy to control – [3]thick

walls wouldn't matter when it comes to connectivity and insiders. It's logical for any data to be stated as secure in

that type of environment, but an authorized/unauthorized "someone" will want to use and abuse it for sure.

[4]VCs often exaggerate to develop a [5]market sector they somehow envision as profitable in the long term,

the real issue is that, while the idea is very marketable, you cannot base future trends on this fact only. They'd better

[6]invest in market segments such as portable security solutions, or risk management companies such as Vontu and

Reconnex, which I covered in a previous post related to [7]insiders abuse.

1. <http://business.timesonline.co.uk/article/0,,9075-2216532.html>

2. [http://www.lyricsfreak.com/j/jamiroquai/deeper+underground\\_20069403.html](http://www.lyricsfreak.com/j/jamiroquai/deeper+underground_20069403.html)

3. <http://ddanchev.blogspot.com/2006/04/would-somebody-please-buy-this-titan-1.html>

4. [http://www.webitpr.com/release\\_detail.asp?ReleaseID=4117](http://www.webitpr.com/release_detail.asp?ReleaseID=4117)
5. <http://ddanchev.blogspot.com/2006/04/spotting-valuable-investments-in.html>
6. <http://ddanchev.blogspot.com/2006/05/valuing-security-and-prioritizing-your.html>
7. <http://ddanchev.blogspot.com/2005/12/insiders-insights-trends-and-possible.html>

364

### **Travel Without Moving - Georgi Markov's KGB Assassination Spot (2006-06-11 16:15)**

In the spirit of the previous [1]hot spot in the Travel Without Moving series, here's another one, this time [2]Georgi

Markov's KGB Assassination spot. [3]Georgi Markov was [4]killed in [5]London, in 1978, using a tiny pellet fired from an [6]umbrella containing 0.2 milligram dose of poison ricin.

You may also find this Time Out's briefing on [7]London's espionage locations interesting.

1. <http://ddanchev.blogspot.com/2006/06/travel-without-moving-kgb-lubyanka.html>

2.

<http://maps.google.com/maps?f=q&hl=en&q=Waterloo+Bridge,+SE1&t=k&om=1&ll=51.506312,-0.114584&spn=0.013543,0.042915>

3. [http://en.wikipedia.org/wiki/Georgi\\_Markov](http://en.wikipedia.org/wiki/Georgi_Markov)
4. <http://www.cnn.com/2003/WORLD/europe/01/07/terror.poison.bulgarian/>
5. <http://news.bbc.co.uk/1/hi/uk/2636459.stm>
6. [http://en.wikipedia.org/wiki/Image:Markov\\_umbrella.PNG](http://en.wikipedia.org/wiki/Image:Markov_umbrella.PNG)
7. <http://www.timeout.com/london/features/340.html>

365

## **It's Getting Cloudy, and Delicious (2006-06-11 16:31)**

[1]For real. A brief summary of the instant links for the last two days :

**01.** [2]Eight Indian Startups to Watch - "Some startups are offering unique solutions for India's burgeoning domestic market, others are targeting global markets. Several are going after both. Red Herring has chosen a few

below-the-radar young companies that we think are worth watching." - to [3]Investing [4]Technology [5]India on

**june 10**

**02.** [6]'Grand Theft Auto' Game Makers Settle With FTC - "A settlement has been reached with the companies behind the popular video game "Grand Theft Auto: San Andreas," Take-Two Interactive and subsidiary Rockstar Games,

which were sued for deceptive practices over hidden sexual content in the game." - to [7]Game [8]Investing on **june 10**

**03.**

[9]Symbian dismisses smartphone security risk - "David Wood, executive vice president of research at

Symbian, said on the Symbian website that smartphones only pose a security risk if companies ignore basic practical

rules." - to [10]Malware [11]Symbian on **june 10**

**04.** [12]AV management 2006 - "We have assembled a comprehensive range from the leading anti-virus prod-

ucts available in today's market. During our testing, we began by checking the capacity of these respective offerings

to cope with basic tasks." - to [13]Security [14]Malware [15]AntiVirus on **june 10**

**05.** [16]Zero-Day Exploits Abound at Legitimate Web Sites - "An exploit distribution network controlled by a

single organization that was using a network of 40 Internet domains, each of which was linked to an average of 500

infected sites, for a total of roughly 20,000 Web pages forwarding the groups' attacks." - to [17]0day

[18]Vulnerabilities on **june 10**

**06.** [19]Taiwan Faces Increasing Cyber Assaults - "A hacker managed to issue an e-mail attachment that con-

tained a fake press release purportedly from the Military Spokesman's Office describing a meeting between People's

First Party representatives and MND officials." - to

[20]InformationWarfare [21]Cyberwarfare [22]Taiwan

[23]China

on **june 10**

**07.** [24]Social- and Interactive-Television Applications Based on Real-Time Ambient-Audio Identification - "We showed how to sample the ambient sound emitted from a TV and automatically determine what is being watched

from a small signature of the sound—all with complete privacy and minuscule effort." - to [25]NewMedia [26]Privacy

[27]Surveillance on **june 10**

**08.** [28]The Evolution of In-Game Ads - "Marketed as a way to help game makers increase their bottom line

or make specific titles more realistic, advertisers are continually searching for ways to reach new audiences— young

males and beyond."- to [29]Game [30]Advertising ... on **june 11**

**09.** [31]Risks of Keeping User Data Outweigh Benefits - "Large data troves are certain to become targets of

hackers, identity thieves and unscrupulous insiders. As the raft of recent data breaches has shown, there are plenty

of companies, organizations and government agencies that do a lousy job at securing data." - to [32]Security on **june 11**

**10.** [33]Protect Me, Protect My Data - "Companies that underestimate security threats to their records do so

at their own peril. It can mean a loss of trust and of business." - to [34]Security on **june 11**

**11.** [35]Audit finds security weaknesses at NASA center - "The IG's audit found other problems as well. Sys-

tem administrators also accessed a key server containing security information without adequate encryption and did not remove unnecessary services from the network." - to [36]Security [37]NASA on **june 11**

366

**12.** [38]America's Most Stolen Vehicles - "The Cadillac Escalade had the highest theft claim rate overall, according to the HLDI, and was the most stolen SUV, according to the CCC 2004 stolen vehicle report." - to [39]Security

[40]Theft on **june 11**

**13.** [41]N Korea in 'US spy plane' warning - "North Korea says it will punish the US, after claiming it is conducting spying flights over its territorial waters." - to [42]Intelligence [43]Reconnaissance on **june 11**

**14.** [44]McAfee SiteAdvisor to add site blocking, extend ratings beyond Web - "McAfee is planning enhance-

ments to its recently acquired SiteAdvisor software that will allow the Web-rating application to block inappropriate

Web sites, offer safety ratings for online transactions and rate Web links that appear in e-mail and IM windows. - to

[45]McAfee [46]SiteAdvisor on **june 11**

**15.** [47]Google and Ebay : The MBA Analysis - "In fact, as they researched the paper over the course of the

year, the authors came to the conclusion that eBay had no choice but to ally with either Yahoo or Microsoft. Then

the Journal reported as much, and the Yahoo/eBay deal went down." - to [48]NewMedia [49]Google [50]Ebay on

## **june 11**

1. <http://del.icio.us/DDanchev?settagview=cloud>
2. <http://www.redherring.com/article.aspx?a=17127>
3. <http://del.icio.us/DDanchev/Investing>
4. <http://del.icio.us/DDanchev/Technology>
5. <http://del.icio.us/DDanchev/India>
6. <http://www.ecommercetimes.com/rsstory/51018.html>
7. <http://del.icio.us/DDanchev/Game>
8. <http://del.icio.us/DDanchev/Investing>
9. <http://www.vnunet.com/vnunet/news/2157916/symbian-dismisses-smartphone>
10. <http://del.icio.us/DDanchev/Malware>
11. <http://del.icio.us/DDanchev/Symbian>
12. <http://www.scmagazine.com/uk/group/test/details/ab23b23f-f6b3-51ca-9609-26a657fc36b7/av+management+2006/>
13. <http://del.icio.us/DDanchev/Security>
14. <http://del.icio.us/DDanchev/Malware>



15. <http://del.icio.us/DDanchev/AntiVirus>
16. <http://www.eweek.com/article2/0,1895,1974779,00.asp>
17. <http://del.icio.us/DDanchev/0day>
18. <http://del.icio.us/DDanchev/Vulnerabilities>
19. <http://www.defensenews.com/story.php?F=1861031&C=asiapac>
20. <http://del.icio.us/DDanchev/InformationWarfare>
21. <http://del.icio.us/DDanchev/Cyberwarfare>
22. <http://del.icio.us/DDanchev/Taiwan>
23. <http://del.icio.us/DDanchev/China>
24. <http://www.mangolassi.org/covell/pubs/euroITV-2006.pdf>
25. <http://del.icio.us/DDanchev/NewMedia>
26. <http://del.icio.us/DDanchev/Privacy>
27. <http://del.icio.us/DDanchev/Surveillance>
28. <http://www.redherring.com/article.aspx?a=17177>
29. <http://del.icio.us/DDanchev/Game>
30. <http://del.icio.us/DDanchev/Advertising>
31. <http://www.ecommercetimes.com/story/WIkqRIxm56uUGb/Risks-of-Keeping-User-Data-Outweigh-Benefits.shtml>
32. <http://del.icio.us/DDanchev/Security>

367

33.

[http://www.businessweek.com/technology/content/jun2006/tc20060608\\_894982.htm](http://www.businessweek.com/technology/content/jun2006/tc20060608_894982.htm)

34. <http://del.icio.us/DDanchev/Security>.

35. [http://www.gcn.com/online/vol1\\_no1/40990-1.html](http://www.gcn.com/online/vol1_no1/40990-1.html)

36. <http://del.icio.us/DDanchev/Security>.

37. <http://del.icio.us/DDanchev/NASA>

38. <http://autos.msn.com/advice/article.aspx?contentid=2891>

39. <http://del.icio.us/DDanchev/Security>.

40. <http://del.icio.us/DDanchev/Theft>

41. <http://news.bbc.co.uk/2/hi/asia-pacific/5068662.stm>

42. <http://del.icio.us/DDanchev/Intelligence>

43. <http://del.icio.us/DDanchev/Reconnaissance>

44.

[http://www.infoworld.com/article/06/06/09/79162\\_HNmcafee\\_rateboost\\_1.html](http://www.infoworld.com/article/06/06/09/79162_HNmcafee_rateboost_1.html)

45. <http://del.icio.us/DDanchev/McAfee>

46. <http://del.icio.us/DDanchev/SiteAdvisor>

47. <http://battellemedia.com/archives/002634.php>

48. <http://del.icio.us/DDanchev/NewMedia>

49. <http://del.icio.us/DDanchev/Google>

50. <http://del.icio.us/DDanchev/Ebay>

368

### **Consolidation, or Startups Popping out Like Mushrooms? (2006-06-13 16:13)**

If technology is the enabler, and the hot commodity these days, spammers will definitely twist the concept of

targeted marketing, while taking advantage of them. Last week I've [1]mentioned the concepts of VoIP, WiFi and Cell phone spam that are slowly starting to take place.

Gartner [2]recently expressed a (pricey) opinion on the upcoming [3]consolidation of spam vendors, while I

feel they totally ignored the technological revolution of spamming to come - IPSec is [4]also said to be dead by 2008..

*" The current glut of anti-spam vendors is about to end, analysts at Gartner said Wednesday. But enterprises*

*shouldn't stay on the sidelines until the shakeout is over. By the end of the year, Gartner predicted, the current*

*roster of about 40 vendors in the enterprise anti-spam filtering market will shrink to fewer than 10. As consolidation accelerates and as anti-spam technology continues to rapidly change, most of today's vendors will be "left by the wayside," said Maurene Caplan Grey, a research director with Gartner, and one of two analysts who authored a*

*recently-released report on the state of the anti-spam market. "*

The consequence of cheap hardware, HR on demand, angel investors falling from the sky on daily basis, and

acquiring vendor licensed IP, would result in start ups popping up like mushrooms to cover the newly developed

market segments, and some will stick it long enough not to get acquired given they realize they poses a core

competency.

Sensor networks, spam traps, bayesian filters, all are holding the front, while we've getting used to "an ac-

ceptable level of spam", not the lack of it. What's emerging for the time being is the next logical stage, that's localized spam on native languages, and believe it or not, its gets through the filters, and impacts productivity, the major

problem posed by spam.

[5]SiteAdvisor - I feel I'm almost acting as an evangelist of the idea - [6]recently responded to [7]Scandoo's

concept, by wisely starting to take advantage of their growing database, and provide the feature in email clients

while protecting against phishing attacks. End users wouldn't consider insecure search by default in order to change

their googling habits, they trust Google more than they would trust an extension, and they'd rather have to worry

about Google abusing their click stream, compared to anything else. [8]Anti-Phishing toolbars are a buzz, and it's nice to see the way they're orbiting around it.

Be a mushroom, don't look for an umbrella from day one!

1. <http://ddanchev.blogspot.com/2006/06/over-performing-spammer.html>
2. <http://www.techweb.com/wire/story/TWB20040317S0009>
3. <http://ddanchev.blogspot.com/2006/04/spotting-valuable-investments-in.html>
4. <http://ddanchev.blogspot.com/2006/02/current-state-of-ip-spoofing.html>
5. <http://ddanchev.blogspot.com/2006/04/spotting-valuable-investments-in.html>
6. <http://www.pcworld.com/news/article/0,aid,126043,00.asp>
7. <http://ddanchev.blogspot.com/2006/05/global-security-challenge-bring-your.html>
8. <http://ddanchev.blogspot.com/2006/03/anti-phishing-toolbars-can-you-trust.html>

369

### **Web Application Email Harvesting Worm (2006-06-13 17:40)**

This is a rare example of a [1]web application vulnerability worm, targeting one of the most popular free email

providers by harvesting emails within their 1GB mailboxes, and of course propagating further.

*" Yahoo! on Monday has repaired a vulnerability in its email service that allowed a worm to harvest email ad-*

*dresses from a user accounts and further spread itself. The JS/Yamanner worm automatically executes when a user*

*opens the message in the Yahoo Mail service. It uses JavaScript to exploit a flaw that until today was unpatched.*

*Yahoo later on Monday fixed the vulnerability. "We have taken steps to resolve the issue and protect our users from further attacks of this worm. The solution has been automatically distributed to all Yahoo! Mail customers, and requires no additional action on the part of the user," Yahoo! spokeswoman Kelley Podboy said in an emailed statement. "*

Web application worms have the potential to dominate the malware threatscape given the amount of traffic

their platforms receive, my point is that even within a tiny timeframe like this, one could achieve speed and efficiency like we've only seen in single-packet worms.

In a previous post related to the "[2]Current State of Web Application Worms", you can also find more com-

ments and resources on the topic. Rather defensive, the content spoofing exploiting the trust between the parties

that I mentioned is nothing compared to the automated harvesting in this case. As there's naturally active research

done in [3]Bluetooth honeypots, IM honeypots, [4]ICQ honeypots, [5]Google Hacking honeypots, it's about time to

start seeding your spam trap emails within free email providers or social networking providers.

The stakes are too high not to be exploited in one way or another, I hope we'll some day get surprised by a

top web property coming up with a fixed vulnerability on their own. Realizing the importance of their emerging

position as attack vector for malware authors is yet another issue to keep in mind. And the best part about web

services is their push patching approach, you're always running the latest version, so relaying on end users is totally

out of the question.

Find out [6]more [7]details on the worm, [8]and [9]comments as well.

**UPDATE:** Rather active month when it comes web application malware events, another [10]Data-Theft Worm

Targets Google's Orkut.

1. <http://www.vnunet.com/vnunet/news/2158123/worm-targets-yahoo-mail>
2. <http://ddanchev.blogspot.com/2006/05/current-state-of-web-application-worms.html>
3. <http://www.f-secure.com/weblog/archives/archive-032006.html#00000836>
4. <http://www.viruslist.com/en/weblog?weblogid=187189654>
5. <http://ghh.sourceforge.net/>



6. <http://www.sarc.com/avcenter/venc/data/js.yamanner@m.html>
7. [http://vil.mcafeesecurity.com/vil/content/v\\_139913.htm](http://vil.mcafeesecurity.com/vil/content/v_139913.htm)
8. <http://isc.sans.org/diary.php?storyid=1398>
9. <http://it.slashdot.org/it/06/06/13/1226209.shtml>
10. [http://blog.spywareguide.com/2006/06/datatheft\\_worm\\_targets\\_google\\_1.html](http://blog.spywareguide.com/2006/06/datatheft_worm_targets_google_1.html)

370

### **No Other Place Like 127.0.0.1 (2006-06-24 04:36)**

Sincere apologies for the sudden disappearance, but thanks for the interest even though I haven't been active

for the last week due to quality offline activities. No other place like 127.0.0.1, and the smell of an untouched

by human hand, Cold War era postage stamps glue on my high value collections - I do own several "stamp anomalies".

Collecting [1]postage stamps is a challenging hobby for a teenager to have, mostly because of his usually low

income, and this rather expensive hobby. The solution in my case back then, was bargaining while reselling ancient

coins and purchasing postage stamps through the margins. While every collection has its story on how I acquired

it, perhaps the most important thing I realized back then was that, if you don't respect something, sooner or later

you're going to lose it to someone with a better attitude towards it.

Posting will resume shortly, a lot has happened for a week, and the only thing I pretend I'm not good at is

wasting my time. As a matter of fact, I've got some very nice comments out of a presentation held at the University

of Dresden, Germany, regarding my [2]Future trends of malware research.

1. [http://en.wikipedia.org/wiki/Postage\\_stamp](http://en.wikipedia.org/wiki/Postage_stamp)

2. <http://wwwse.inf.tu-dresden.de/wiki/images/f/f6/PRO-TimLackorzynski.pdf>

371

## **Travel Without Moving - Erasmus Bridge (2006-06-25 18:33)**

Catching up with last week's [1]Travel Without Moving shot, [2]this one isn't intelligence of military related, but a

marvelous engineering achievement, [3]Erasmus Bridge – perhaps the perfect moment to demonstrate my amateur

photographer skills while tripping around. I will definitely share more shots from cons and life, the way I experience

it, anytime now. And meanwhile, you can take a peek at the latest addition to the [4]Eyeball Series, the [5]North

Korean Missile Launch Furor – catching up with a [6]conventional weaponry doctrine is anything else but a milestone.

Google Earth and Google Maps continue making the headlines as [7]a "threat" to national security, where the key points remain the balancing of satellite reconnaissance capabilities between developed and developing nations, the freshness of the data, and it's [8]quality. Sensitive locations can indeed be spotted, and then again, so what?

And, with [9]the [10]launch of Geoportail.fr the French government aims at achieving transparency, rather than [11]overhyping this common sense "insecurity".

1. <http://ddanchev.blogspot.com/2006/06/travel-without-moving-georgi-markovs.html>

2. [http://maps.google.com/maps?f=q&hl=en&q=Erasmus+Bridge&ie=UTF8&am;am;t=k&om=0&ll=51.909107,4.48667&spn=0.](http://maps.google.com/maps?f=q&hl=en&q=Erasmus+Bridge&ie=UTF8&am;am;t=k&om=0&ll=51.909107,4.48667&spn=0.008048,0.019312)

[008048,0.019312](http://maps.google.com/maps?f=q&hl=en&q=Erasmus+Bridge&ie=UTF8&am;am;t=k&om=0&ll=51.909107,4.48667&spn=0.008048,0.019312)

3. [http://en.wikipedia.org/wiki/Erasmus\\_Bridge](http://en.wikipedia.org/wiki/Erasmus_Bridge)

4. <http://www.eyeball-series.org/>

5. <http://cryptome.org/dprk-furor/dprk-eyeball.htm>

6. <http://ddanchev.blogspot.com/2006/02/who-needs-nuclear-weapons-anymore.html>

7. <http://ddanchev.blogspot.com/2006/04/threat-by-google-earth-has-just.html>

8.

<http://www.informationweek.com/software/showArticle.jhtml?articleID=189500473&subSection=Enterprise+Applica>

[tions](#)

9. [http://www.wired.com/news/technology/internet/0,71234-0.html?tw=wn\\_technology\\_1](http://www.wired.com/news/technology/internet/0,71234-0.html?tw=wn_technology_1)

10.

<http://edition.cnn.com/2006/TECH/internet/06/23/france.google.earth.reut/index.html>

11. <http://www.csmonitor.com/2005/1201/p13s01-stct.html>

372

## **Delicious Information Warfare - 13/24 June (2006-06-25 19:41)**

Brief summaries of key events for the last week and a half, catch up with [1]previous ones as well. I intend to continue sharing my daily reads while emphasizing on the big picture, and emerging trends. [2]Great quote courtesy of the

The Royal Swedish Academy of War Sciences : *"The world isn't run by weapons anymore, or energy, or money. It's*

*run by little ones and zeros, little bits of data. It's all just electrons. . . . There's a war out there . . . and it's not about who's got the most bullets. It's about who controls the information. What we see and hear, how we work, what we think, it's all about information. "*

**01.** [3]Eyeballing North Korean Missile Launch Furor - "Latest satellite photo coverage and description of the

launch site facilities." to [4]Military [5]Satellite  
[6]Reconnaissance [7]GEOINT ... **on 25 June**

## **02.**

[8]VoIP wiretapping could lead to more problems -  
"Requiring Internet service providers to respond in

real time to requests for them to record VoIP calls would  
open up the Internet to new vulnerabilities, Whitfield Diffie

added." to [9]Intelligence [10]Terrorism [11]Wiretapping  
[12]CALEA [13]VoIP **on 25 June**

**03.** [14]Police arrest two in Japan data theft case -  
"Blackmailers attempted to extort almost \$90,000 from

one of Japan's largest phone companies by threatening to  
reveal a leak of private data belonging to four million

customers before a major shareholder meeting." to  
[15]Espionage [16]Insider [17]Investing **on 25 June**

**04.** [18]Kevin Mitnick, the great pretender - "ZDNet UK  
caught up with the ex-cracker to discuss developments in  
social engineering, new U.S. laws monitoring telephone  
systems and alleged "NASA hacker" Gary McKinnon's

impending extradition to the United States." to [19]Security  
[20]Interview **on 25 June**

**05.** [21]Data-Theft Worm Targets Google's Orkut - "Now,  
however, the infection will pop up a message telling

you your data is being mailed off someplace, before sending  
you to the Orkut site." to [22]Malware [23]Web **on 25**

**June**

**06.** [24]French Microsoft Web site hacked - "Hackers on Sunday broke into a part of Microsoft's French Web

site, replacing the front page with online graffiti." to [25]Hacktivism [26]Microsoft [27]Defacement **on 25 June**

**07.** [28]SCADA industry debates flaw disclosure - "The guys who are setting up these systems are not security professionals. And many of the systems that are running SCADA applications were not designed to be secure—it's a hacker's playground."

to [29]Security [30]SCADA [31]Cyberterrorism [32]Vulnerabilities **on 25 June**

**08.** [33]Details emerge on second potential NSA facility - "The room had a sophisticated set of double secu-

rity doors, known as a "mantrap," and any engineer who worked inside required extensive security clearances." to

[34]Intelligence [35]NSA [36]Terrorism [37]Surveillance [38]Wiretapping **on 25 June**

**09.** [39]Next-Gen Bank Trojans Are Upon Us - "The 3G Banking Trojan can steal your info and then siphon

your account of its cash. The 3G Banking Trojan began with the "Win32.Grams" piece of malware, which first

appeared in 2004."to [40]Malware **on 25 June**

**10.** [41]Malware authors eyeing Web-based applications - "As Web-based services grow increasingly popular,

industry experts say users should brace for more of these threats." to [42]Malware [43]Web **on 25 June**

## 11.

[44]Stratcom leads DOD cyberdefense efforts -

“Unfortunately for us, cyberterrorism is cheap, and it’s

fast,” Kehler said. “Today’s terrorist moves at the speed of information.” to [45]Defense [46]InformationWarfare

[47]Cyberterrorism **on 25 June**

373

**12.** [48]Text Messaging Used as Malware Lure - "Botnet herders have found a crafty new way to lure computer users to maliciously rigged Web sites—via text messaging on cell phones." to [49]Malware [50]Mobile **on 25**

**June**

**13.** [51]Two China Search Sites Shut - "Censorship or maintenance? That’s the question after two Chinese

search engines shut down temporarily." to [52]China [53]Censorship [54]FreeSpeech **on 25 June**

**14.** [55]Web services increasingly under attack - "As larger audiences flock to Web sites that run on ever more powerful programming scripts, malware writers are them fertile ground." to [56]Security [57]Malware [58]Web **on 25 June**

**15.** [59]What’s the Endpoint of Endpoint Security? -

"Finally, there’s a more manipulative progenitor of new

jargon: the analyst community. White papers, market reports and mystical squares can get crowded, and the big

vendors often dominate them."

to [60]Security [61]Investing [62]Advertising  
[63]Leadership **on 25 June**

**16.** [64]Expatriates in Canada pressured to spy - "Despite strong warnings from the government of Canada,

certain countries continue to use their intelligence services to manipulate and exploit expatriate communities in

Canada," CSIS said." to [65]Intelligence [66]OSINT  
[67]Espionage **on 25 June**

**17.** [68]Review: Terror On The Internet - "Terror on the Internet" usefully outlines the basic contours of his subject, giving a taste of Al Qaeda's Internet rhetoric and strategies, along with those of less well-known militant

groups from Colombia to the Basque country to Chechnya." to [69]InformationWarfare [70]Cyberterrorism [71]Ter-

rorism [72]PSYOPS **on 25 June**

**18.** [73]Web of terror - "The suspects reportedly became radicalized through militant Web sites and received

online advice from Younis Tsouli, the Britain-based Webmaster for Islamic extremist sites who called himself

"Terrorist 007," before he was arrested late last year." to [74]InformationWarfare [75]Cyberterrorism [76]Terrorism

[77]PSYOPS [78]Web **on 25 June**

1. <http://ddanchev.blogspot.com/2006/06/its-getting-cloudy-and-delicious.html>

2. [http://www.slis.indiana.edu/news/story.php?story\\_id=549](http://www.slis.indiana.edu/news/story.php?story_id=549)



3. <http://cryptome.org/dprk-furor/dprk-eyeball.htm>
4. <http://del.icio.us/DDanchev/Military>
5. <http://del.icio.us/DDanchev/Satellite>
6. <http://del.icio.us/DDanchev/Reconnaissance>
7. <http://del.icio.us/DDanchev/GEOINT>
8. <http://www.techworld.com/security/news/index.cfm?newsID=6213&pagtype=all>
9. <http://del.icio.us/DDanchev/Intelligence>
10. <http://del.icio.us/DDanchev/Terrorism>
11. <http://del.icio.us/DDanchev/Wiretapping>
12. <http://del.icio.us/DDanchev/CALEA>
13. <http://del.icio.us/DDanchev/VoIP>
14. <http://www.vnunet.com/vnunet/news/2158327/arrests-japan-extortion-case>
15. <http://del.icio.us/DDanchev/Espionage>
16. <http://del.icio.us/DDanchev/Insider>
17. <http://del.icio.us/DDanchev/Investing>
18. [http://news.com.com/2008-1029\\_3-6083668.html](http://news.com.com/2008-1029_3-6083668.html)
19. <http://del.icio.us/DDanchev/Security>
20. <http://del.icio.us/DDanchev/Interview>

21. [http://blog.spywareguide.com/2006/06/datatheft\\_worm\\_targets\\_google\\_1.html](http://blog.spywareguide.com/2006/06/datatheft_worm_targets_google_1.html)
22. <http://del.icio.us/DDanchev/Malware>
23. <http://del.icio.us/DDanchev/Web>
24. [http://news.com.com/2100-7349\\_3-6085589.html](http://news.com.com/2100-7349_3-6085589.html)
25. <http://del.icio.us/DDanchev/Hacktivism>
26. <http://del.icio.us/DDanchev/Microsoft>
27. <http://del.icio.us/DDanchev/Defacement>
28. <http://www.securityfocus.com/news/11396>
29. <http://del.icio.us/DDanchev/Security>
30. <http://del.icio.us/DDanchev/SCADA>
31. <http://del.icio.us/DDanchev/Cyberterrorism>
32. <http://del.icio.us/DDanchev/Vulnerabilities>
33. <http://www.securityfocus.com/brief/234>
34. <http://del.icio.us/DDanchev/Intelligence>
35. <http://del.icio.us/DDanchev/NSA>
36. <http://del.icio.us/DDanchev/Terrorism>
37. <http://del.icio.us/DDanchev/Surveillance>
38. <http://del.icio.us/DDanchev/Wiretapping>

39. <http://www.internetnews.com/security/article.php/3615631>
40. <http://del.icio.us/DDanchev/Malware>
41. [http://searchsecurity.techtarget.com/originalContent/0,289142,sid14\\_gci1195528,00.html](http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1195528,00.html)
42. <http://del.icio.us/DDanchev/Malware>
43. <http://del.icio.us/DDanchev/Web>
44. <http://www.fcw.com/article94954-06-19-06-Web>
45. <http://del.icio.us/DDanchev/Defense>
46. <http://del.icio.us/DDanchev/InformationWarfare>
47. <http://del.icio.us/DDanchev/Cyberterrorism>
48. <http://www.eweek.com/article2/0,1759,1980932,00.asp?kc=EWRSS03129TX1K0000614>
49. <http://del.icio.us/DDanchev/Malware>
50. <http://del.icio.us/DDanchev/Mobile>
51. <http://www.redherring.com/Article.aspx?a=17315&hed=Two+China+Search+Sites+Shut>
52. <http://del.icio.us/DDanchev/China>
53. <http://del.icio.us/DDanchev/Censorship>
54. <http://del.icio.us/DDanchev/FreeSpeech>

55. [http://www.businessweek.com/ap/financialnews/D8IE2SCG1.htm?sub=apn\\_tech\\_up&chan=tc](http://www.businessweek.com/ap/financialnews/D8IE2SCG1.htm?sub=apn_tech_up&chan=tc)
56. <http://del.icio.us/DDanchev/Security>
57. <http://del.icio.us/DDanchev/Malware>
58. <http://del.icio.us/DDanchev/Web>
59. <http://www.csoonline.com/alarmed/>
60. <http://del.icio.us/DDanchev/Security>
61. <http://del.icio.us/DDanchev/Investing>
62. <http://del.icio.us/DDanchev/Advertising>
63. <http://del.icio.us/DDanchev/Leadership>
64. <http://news.scotsman.com/latest.cfm?id=921822006>
65. <http://del.icio.us/DDanchev/Intelligence>
66. <http://del.icio.us/DDanchev/OSINT>
67. <http://del.icio.us/DDanchev/Espionage>
68. <http://www.iht.com/articles/2006/06/23/arts/idbriefs24c.php>
69. <http://del.icio.us/DDanchev/InformationWarfare>
70. <http://del.icio.us/DDanchev/Cyberterrorism>
- 375
71. <http://del.icio.us/DDanchev/Terrorism>

- 72. <http://del.icio.us/DDanchev/PSYOPS>
- 73. [http://seattletimes.nwsources.com/html/opinion/2003081872\\_sundayjihad25.html](http://seattletimes.nwsources.com/html/opinion/2003081872_sundayjihad25.html)
- 74. <http://del.icio.us/DDanchev/InformationWarfare>
- 75. <http://del.icio.us/DDanchev/Cyberterrorism>
- 76. <http://del.icio.us/DDanchev/Terrorism>
- 77. <http://del.icio.us/DDanchev/PSYOPS>
- 78. <http://del.icio.us/DDanchev/Web>

376

### **World's Internet Censorship Map (2006-06-26 00:16)**

While it seems rather quiet on the [1]Internet's censorship front, the media coverage on the topic represents a cyclical buzz that reemerges with the time.

Thankfully, initiatives as the [2]OpenNet one, and organizations such as [3]Reporters Without Borders never stop being the society's true watchdogs when it comes to Internet censorship. ONI's neat [4]visualization of the

Internet filtering map is a great way of pin pointing key locations, and provide further details through their [5]in-depth reports, take a look for yourself!

Censorship is capable of [6]running entire governments, maintaining [7]historical political power, and mostly

ruling by "[8]excluding the middle". Recently, two of [9]China's leading Internet portals were shut down due

to maintenance issues acting as the excuse for improving their filtering capabilities. Reporters Without Borders

conducted an [10]outstanding analysis of the situation, coming to the conclusion " *that the search engines of*

*China's two leading Internet portals, [11] Sina and [12] Sohu, after they were shut down from 19 to 21 June for what they described as a "technical upgrade" but which in fact was designed to improve the filtering of their search results.*

What is Google up to? Making [13]business compromises in order to harness the power of the growing Chi-

nese Internet population. And while [14]the Wall is cracking from within, the world is also taking actions against the

fact that there're currently [15]30 journalists behind bars in China.

1. <http://www.google.com/trends?q=Censorship>
2. <http://www.opennetinitiative.net/>
3. <http://www.rsf.org/>
4. <http://opennet.net/map/>
5. <http://www.opennetinitiative.net/modules.php?op=modload&name=Archive&file=index&req=viewarticle&artid=1>
6. <http://ddanchev.blogspot.com/2006/04/securing-political-investments-through.html>

7. <http://ddanchev.blogspot.com/2006/02/chinese-internet-censorship-efforts.html>
8. <http://www.cjr.org/issues/2006/3/schulman.asp>
9. <http://www.redherring.com/Article.aspx?a=17315&hed=Two+China+Search+Sites+Shut>
10. [http://www.rsf.org/article.php3?id\\_article=18015](http://www.rsf.org/article.php3?id_article=18015)
11. <http://www.sina.com.cn/>
12. <http://www.sohu.com/>
13. <http://edition.cnn.com/2006/TECH/internet/06/07/google.censorship.ap/>
14. <http://www.forbes.com/business/global/2006/0227/018A.html>
15. <http://www.interfax.cn/showfeature.asp?aid=13850&slug=INTERNET-CENSORSHIP>

377

### **Big Brother in the Restroom (2006-06-26 01:09)**

Wikes! This is nasty, and while the porn industry has commercialized the idea a long time ago, I never imagined

the levels of crime in public restrooms would "reach" levels requiring CCTVs to be installed – if there's so much vandalism going on in public restrooms, these will definitely get stolen as well, picture the situation! [1]Norway

installs surveillance cameras in park restrooms.

**Hint** : once you get involved in the [2]CCTV irony, I say irony mainly because the dude behind the 40 motion

detection and face recognition wall is having another CCTV behind his back, you end up spending tax payers money

to cover "blind spots", and end up with a negative ROI while trying to achieve self-regulation, if one matters!

[3]Surveillance and Society's journal still remains the most resourceful publication on surveillance studies and

its impact on society.

Further reading and previous cases:

[4]The Hidden Camera

[5]Iowa Judge Says Hidden Restroom Camera Case Can Proceed to Trial

1. <http://msnbc.msn.com/id/13438209/>
2. [http://billcaldwell.com/acatalog/21\\_8\\_01.gif](http://billcaldwell.com/acatalog/21_8_01.gif)
3. <http://www.surveillance-and-society.org/>
4. [http://www.csoononline.com/read/090105/hiddencamera\\_3824.html](http://www.csoononline.com/read/090105/hiddencamera_3824.html)
5. <http://www.insurancejournal.com/news/midwest/2006/05/23/68750.htm>



## **Dealing with Spam - The O'Reilly.com Way (2006-06-26 15:23)**

While China feels that centralization is the core of everything, and is [1]licensing the use of mail servers to fight

spam, thus totally ignoring the [2]evolution of spam techniques, the other day I came across to some recent [3]Spam

Statistics from Oreilly.com – scary numbers!

*" Our mail servers accepted 1,438,909 connections, attempting to deliver 1,677,649 messages.*

*We rejected*

*1,629,900 messages and accepted only 47,749 messages. That's a ratio of 1:34 accepted to rejected messages! Here*

*is how the message rejections break down:*

*Bad HELO syntax: 393284*

*Sending mail server masquerades as our mail server: 126513*

*Rejected dictionary attacks: 22567*

*Rejected by SORBS black list: 262967*

*Rejected by SpamHaus black list: 342495*

*Rejected by local block list: 5717*

*Sender verify failed: 4525*

*Recipient verify failed (bad To: address): 287457*

*Attempted to relay: 5857*

*No subject: 176*

*Bad header syntax: 0*

*Spam rejected (score => 10): 42069*

*Viruses/malware rejected: 2575*

*Bad attachments rejected: 1594"*

Draw up the conclusions for yourself, besides shooting into the dark or general syntax errors, total waste of

email traffic resulting in delayed email is the biggest downsize here, thankfully, non-commercial methods are still

capable of dealing with the problem. At the bottom line, sending a couple of million email messages on the cost of

anything, and getting a minor response from a "Hey this is hell of a deal and has my username on the top of it!" type of end users seems to keep on motivating the sender. Localized spam is much more effective as an idea, but much

easier to trace compared to mass-marketing approaches, though I feel it would emerge with the time.

Browse through [4]Spamlinks.net for anything anti-spam related, quite an amazing resource.

1. <http://ddanchev.blogspot.com/2006/04/fighting-internets-email-junk-through.html>

2. <http://ddanchev.blogspot.com/2006/06/over-performing-spammer.html>

3. [http://radar.oreilly.com/archives/2006/06/spam\\_filtering\\_statistics\\_from.html](http://radar.oreilly.com/archives/2006/06/spam_filtering_statistics_from.html)

4. <http://spamlinks.net/>

379

### **Shots From the Wild - Terrorism Information Awareness Program Demo Portal (2006-06-27 03:54)**

A lot has changed since my last post on "[1]Data mining, terrorism and security", namely [2]NSA's warrantless

surveillance efforts. So, in the spirit of a [3]second possible NSA facility, I've decided to post a shot from the [4]TIA's early stages of development obtained through the most detailed, conceptual, and from a developer's point of view

[5]description of the program.

There've also been speculations on the severity of NSA wiretapping program compared to the [6]Watergate

scenario, while I feel that besides political engineering through [7]infowar, it also occurs relatively more often over a juicy barbecue.

Related resources on [8]Intelligence, [9]NSA, [10]Surveillance, [11]Wiretapping.

1. <http://ddanchev.blogspot.com/2006/03/data-mining-terrorism-and-security.html>

2. [http://en.wikipedia.org/wiki/NSA\\_warrantless\\_surveillance\\_controversy](http://en.wikipedia.org/wiki/NSA_warrantless_surveillance_controversy)
3. <http://www.securityfocus.com/brief/234>
4. [http://en.wikipedia.org/wiki/Total\\_Information\\_Awareness](http://en.wikipedia.org/wiki/Total_Information_Awareness)
5. <http://www.epic.org/privacy/profiling/tia/tiasystemdescription.pdf>
6. [http://www.wired.com/news/technology/0,71227-0.html?tw=wn\\_technology\\_1](http://www.wired.com/news/technology/0,71227-0.html?tw=wn_technology_1)
7. [http://photos1.blogger.com/blogger/1933/1779/1600/information\\_warfare.1.gif](http://photos1.blogger.com/blogger/1933/1779/1600/information_warfare.1.gif)
8. <http://del.icio.us/DDanchev/Intelligence>
9. <http://del.icio.us/DDanchev/NSA>
10. <http://del.icio.us/DDanchev/Surveillance>
11. <http://del.icio.us/DDanchev/Wiretapping>

380

### **Malicious Web Crawling (2006-06-27 17:34)**

SiteAdvisor indeed cashed for [1]evaluating the maliciousness of the web, and New Zealand feels that [2]nation wide

google hacking initiatives are a more feasible solution to the problem of google hacking, compared to the Catawba

County Schools Board of Education who blamed [3]Google for indexing student test scores & social security numbers.

It's like having a just-moved, 25/30 years old neighbors next to your place, who didn't know you have [4]thermal

movement detection equipment and [5]parabolic microphones, in order to seal the house by using robots.txt, or

assigning the necessary permissions on the web server asap.

Tip to the Board of Education, don't bother Google but take care of the problem on your own, immediately,

[6]through [7]Google's automatic URL removal system, by first " *inserting the appropriate meta tags into the page's HTML code. Doing this and submitting via the automatic URL removal system will cause a temporary, 180-day*

*removal of these pages from the Google index, regardless of whether you remove the robots.txt file or meta tags*

*after processing your request. "*

Going back to the idea of malicious web crawling, the best "what if" analysis comes from [8]Michal Zalewski,

back in 2001's Phrack issue article on "[9]The Rise of the Robots" - nice starting quote! It tries to emphasize that

" *Others - Internet workers - hundreds of never sleeping, endlessly browsing information crawlers, intelligent agents, search engines... They come to pick this information, and - unknowingly - to attack victims. You can stop one of*

*them, but can't stop them all. You can find out what their orders are, but you can't guess what these orders will be tomorrow, hidden somewhere in the abyss of not yet explored cyberspace. Your private army, close at hand, picking*

*orders you left for them on their way. You exploit them without having to compromise them. They do what they are*

*designed for, and they do their best to accomplish it. Welcome to the new reality, where our A.I. machines can rise*

*against us. "*

That's a far more serious security issue to keep an eye on, instead of Google's crawlers eating your web site

for breakfast.

1. <http://ddanchev.blogspot.com/2006/02/look-whos-gonna-cash-for-evaluating.html>
2. <http://ddanchev.blogspot.com/2006/05/nation-wide-google-hacking-initiative.html>
3. <http://blog.searchenginewatch.com/blog/060626-085140>
4. <http://www.freshpatents.com/Thermal-movement-sensor-dt20060223ptan20060039442.php?type=description>
5. [http://en.wikipedia.org/wiki/Parabolic\\_microphone](http://en.wikipedia.org/wiki/Parabolic_microphone)
6. <http://www.google.com/support/webmasters/bin/answer.py?answer=35303>
7. <http://services.google.com/urlconsole/controller>

8. <http://lcamtuf.coredump.cx/>

9. <http://www.phrack.org/show.php?p=57&a=10>

381

## **Delicious Information Warfare - 24/27 June (2006-06-28 02:35)**

Go through my daily reads for [1]13/24 June as well.

**01.** [2]Meteorite Collision - "Japanese animation showing what would happen if a giant meteor hit the Earth."

to [3]Space **on june 25**

**02.** [4]Should We Lift North Korean Sanctions? - "Quentin Hardy summed up his side's argument: "Capitalism

has corrupted other authoritarian regimes, why not North Korea?" to [5]Investing **on june 25**

**03.** [6]The ABCs of New Security Leadership - "Maintaining the right level of boardroom and employee aware-

ness is a consequence of leadership. And more effective ideas and tactics are replacing the old, reactive security

leadership paradigm. Below, CSO looks at what's Out and what's In." to [7]Security [8]Leadership **on june 27**

**04.** [9]Blackmailer : the story of Gpcode - "Analysts at Kaspersky Lab had successfully cracked a 660 bit RSA encryption key. This was the latest victory against a cyber blackmailer that had been plaguing users in Russia for over

a year and a half." to [10]Malware [11]Ransomware **on june 27**

**05.** [12]My Anti-Virus Revolving Door - "I'm the Donald Trump of anti-virus software testing. It won't be long before they're all fired." to [13]Malware [14]AntiVirus **on june 27**

**06.** [15]Eyeballing Israel Signal Facilities - "Israeli Signal Facilities, courtesy of the Eyeball Series." to [16]Security [17]Defense [18]Reconnaissance [19]Satellite [20]GEOINT **on june 27**

**07.** [21]DHS Special Report Can DHS meet IT cybersecurity expectations? - "In the Defense budget we have

put hundreds of millions of dollars in for info. dominance," Weldon said. He cited Pentagon programs to fund

universities to launch cybersecurity studies centers and to expand the military's own cybersecurity programs." to

[22]Security [23]Defense [24]Cyberterrorism [25]Leadership **on june 27**

**08.** [26]Tampa GOP Cyber-Attack - "As the global Islamist war heats up, technically savvy cyber-terrorists will continue to look to find weaknesses in the Internet infrastructure of the West." to [27]InformationWarfare [28]Cyberterrorism [29]Hacktivism [30]PSYOPS **on june 27**

**09.** [31]Analysis Warns U.S. of Cyber Security Weaknesses - "If our nation is hit by a cyber Katrina that wipes out large parts of the Internet, there is no coordinated plan in place to restart and restore the Internet," said John J.

Castellani, President of the Roundtable." to [32]Security [33]Defense [34]Cyberterrorism [35]Leadership **on june 27**

**10.** [36]Ignoring the Great Firewall of China - "The so-called "Great Firewall of China" operates, in part, by inspecting TCP



packets for keywords that are to be blocked. If the keyword is present, TCP reset packets (viz: with

the RST flag set) are sent to both endpoints of the connection.." to [37]Censorship [38]China [39]FreeSpeech **on june 27**

**11.**

[40]Encyclopedia of Espionage, Intelligence, and Security - "Espionage information." to [41]Intelligence

[42]Espionage **on june 27**

**12.** [43]China-Led Group to Fight Web Fraud, Cyber Terrorism - "A Russian and Chinese-led bloc of Asian states said Thursday it plans to set up an expert group to boost computer security and help guard against threats to their regimes from the Internet." to [44]Security **on june 27**

**13.** [45]Immunizing The Internet, Or : How I Learned To Stop Worrying And Love The Worm - "In a 1997 ex-

ercise, NSA teams hacked into computer systems at four regional military commands and the National Military

382

Command Center and showed that hackers could cause large-scale power outages and 911 emergency telephone network overloads." to [46]Security [47]Defense [48]InformationWarfare [49]Cyberterrorism **on june 27**

**14.** [50]Five Questions For Martin Roesch, Founder and CTO of Sourcefire - "In 1998, Roesch created Snort,

an app that sniffs out malicious traffic trying to enter a network. Snort's free source code has been downloaded

more than 3 million times." to [51]Interview **on june 27**

**15.** [52]Firms Eye Video Surveillance - "And as the technology shrinks, the cameras slip deeper into the background, hardly noticed, streaming more than 4 billion hours of footage a week—footage that usually ends up lost,

and never seen." to [53]Surveillance [54]CCTV [55]Technology **on june 27**

**16.** [56]How big is Earth compared to other planets and stars? - "Fun series of photos comparing Earth's size to that of other planets and stars." to [57]Space **on june 27**

**17.** [58]All-Seeing Blimp on the Rise - "The problem with the American military today is that it doesn't have a giant, robotic airship, two-and-a-half times the size of the Goodyear blimp, that can watch over an entire city at

once. The idea is to park an unmanned airship over a hot zone. to [59]Military [60]Surveillance [61]Privacy **on june 27**

**18.** [62]Malware in Popular Networks - "Some of the other popular means of computer supported collabora-

tion are USENET, IRC, P2P, IM. We have seen a consistent uprise of malware targeting these collaborative systems."

to [63]Malware **on june 27**

**19.**

[64]Word macro trojan dropper and (another) downloader -  
"We've seen a lot of new malware being

spammed in last couple of hours." to [65]Malware **on june**  
**27**

1. <http://ddanchev.blogspot.com/2006/06/delicious-information-warfare-1324.html>
2. [http://www.ursispaltenstein.ch/blog/weblog.php?weblog/teorite\\_collision/](http://www.ursispaltenstein.ch/blog/weblog.php?weblog/teorite_collision/)
3. <http://del.icio.us/DDanchev/Space>
4. [http://blogs.forbes.com/digitalrules/2006/06/should\\_we\\_lift\\_.html](http://blogs.forbes.com/digitalrules/2006/06/should_we_lift_.html)
5. <http://del.icio.us/DDanchev/Investing>
6. [http://www.csoononline.com/fundamentals/abc\\_leadership.html](http://www.csoononline.com/fundamentals/abc_leadership.html)
7. <http://del.icio.us/DDanchev/Security>
8. <http://del.icio.us/DDanchev/Leadership>
9. <http://www.viruslist.com/en/analysis?pubid=189678219>
10. <http://del.icio.us/DDanchev/Malware>
11. <http://del.icio.us/DDanchev/Ransomware>
12. <http://www.eweek.com/article2/0,1895,1982068,00.asp>
13. <http://del.icio.us/DDanchev/Malware>

14. <http://del.icio.us/DDanchev/AntiVirus>
15. <http://cryptome.org/ilsig-eyeball.htm>
16. <http://del.icio.us/DDanchev/Security>
17. <http://del.icio.us/DDanchev/Defense>
18. <http://del.icio.us/DDanchev/Reconnaissance>
19. <http://del.icio.us/DDanchev/Satellite>
20. <http://del.icio.us/DDanchev/GEOINT>
21. [http://www.gcn.com/print/25\\_17/41093-1.html](http://www.gcn.com/print/25_17/41093-1.html)
22. <http://del.icio.us/DDanchev/Security>
23. <http://del.icio.us/DDanchev/Defense>
24. <http://del.icio.us/DDanchev/Cyberterrorism>
25. <http://del.icio.us/DDanchev/Leadership>

383

26. <http://frontpagemagazine.com/Articles/ReadArticle.asp?ID=22785>
27. <http://del.icio.us/DDanchev/InformationWarfare>
28. <http://del.icio.us/DDanchev/Cyberterrorism>
29. <http://del.icio.us/DDanchev/Hacktivism>
30. <http://del.icio.us/DDanchev/PSYOPS>
31. [http://www.govtech.net/magazine/channel\\_story.php/10001](http://www.govtech.net/magazine/channel_story.php/10001)

2

- 32. <http://del.icio.us/DDanchev/Security>
- 33. <http://del.icio.us/DDanchev/Defense>
- 34. <http://del.icio.us/DDanchev/Cyberterrorism>
- 35. <http://del.icio.us/DDanchev/Leadership>
- 36. <http://www.cl.cam.ac.uk/~rnc1/ignoring.pdf>
- 37. <http://del.icio.us/DDanchev/Censorship>
- 38. <http://del.icio.us/DDanchev/China>
- 39. <http://del.icio.us/DDanchev/FreeSpeech>
- 40. <http://www.espionageinfo.com/>
- 41. <http://del.icio.us/DDanchev/Intelligence>
- 42. <http://del.icio.us/DDanchev/Espionage>
- 43. <http://www.technewsworld.com/story/W8Hy0zsX6GC9iy/China-Led-Group-to-Fight-Web-Fraud-Cyber-Terrorism.xhtm>

1

- 44. <http://del.icio.us/DDanchev/Security>
- 45. [http://www.harvardlawreview.org/issues/119/june06/note/immunizing\\_the\\_internet.pdf](http://www.harvardlawreview.org/issues/119/june06/note/immunizing_the_internet.pdf)
- 46. <http://del.icio.us/DDanchev/Security>

47. <http://del.icio.us/DDanchev/Defense>
48. <http://del.icio.us/DDanchev/InformationWarfare>
49. <http://del.icio.us/DDanchev/Cyberterrorism>
50. <http://www.informationweek.com/news/showArticle.jhtml?articleID=189500016>
51. <http://del.icio.us/DDanchev/Interview>
52. <http://www.redherring.com/Article.aspx?a=17371&hed=Firms+Eye+Video+Surveillance%0D%0A>
53. <http://del.icio.us/DDanchev/Surveillance>
54. <http://del.icio.us/DDanchev/CCTV>
55. <http://del.icio.us/DDanchev/Technology>
56. <http://www.rense.com/general72/size.htm>
57. <http://del.icio.us/DDanchev/Space>
58. <http://defensetech.military.com/archives/002541.html>
59. <http://del.icio.us/DDanchev/Military>
60. <http://del.icio.us/DDanchev/Surveillance>
61. <http://del.icio.us/DDanchev/Privacy>
62. [http://www.mcafee.com/us/local\\_content/white\\_papers/threat\\_center/wp\\_dmitrygryaznov\\_vb2005.pdf](http://www.mcafee.com/us/local_content/white_papers/threat_center/wp_dmitrygryaznov_vb2005.pdf)
63. <http://del.icio.us/DDanchev/Malware>

64. <http://isc.sans.org/diary.php?storyid=1447&isc=4da9a5a6ffa3426c34d3e2c501f1125c>

65. <http://del.icio.us/DDanchev/Malware>

384

## **Tracking Down Internet Terrorist Propaganda (2006-06-29 03:27)**

I always knew there's a team of cheap marketers behind every terrorist organization trying to market yet another

multimedia killing, or put it simple fear, treats, and no respect for life. Why cheap? Mainly because there's no

segmentation or niche issues to deal with, but mostly mass marketing, while harnessing the power of the never

ending resonation from the media echo.

Rather biased, today's opinion on [1]Cyberterrorism always has to do primarily with destruction as the core of

the problem. Active research is already conducted on "[2]Arabic Extremist Group Forum Messages' Characteristics"

and "[3]Terrorist Social Network Analysis", and the real issues still remain **communication, research, fundraising, propaganda, recruitment** and **training** – I wish [4]Dorothy Denning was also blogging on the topic!

iDefense, being the [5]masters of [6]CYBERINT, recently [7]found jihadist web sites related to Zarqawi's "Suc-

cessor". The interesting part :

*" This website contains forums with a mix of threads covering items from the latest information on the mili-*

*tants in the Middle East, such as a video of militants in Syria, to hacker education, such as Microsoft Word documents available for downloading that detail CGI, unicode and php exploits. The members appear to be interested in physical and cyber-related threats. The membership of the site is growing and is already over 10,000+ members. Plus, we at*

*iDefense/VeriSign are very interested to see what hacking issues or levels of cyber expertise may be covered on this site. "*

By the way, I just came across to an outstanding [8]list of Islamic sites at [9]Cryptome. These are definitely

about to get crawled, analyzed, and for sure, [10]under attack in the future. For instance, the most recent example

of [11]hacktivism tensions, are the [12]hundreds of hacked Israeli web pages, in the light of Israel's military action in Gaza.

Further reading on:

[13]Terrorism

[14]Cyberterrorism

[15]How Modern Terrorism Uses the Internet

[16]Jihad Online : Islamic Terrorists and the Internet

[17]Right-wing Extremism on the Internet

[18]Terrorist web sites courtesy of the [19]SITE Institute



[20]The HATE [21]Directory November 2005 update

[22]Recruitment by Extremist Groups on the Internet

1. <http://ddanchev.blogspot.com/2006/05/techno-imperialism-and-effect-of.html>
2. <http://ddanchev.blogspot.com/2006/05/arabic-extremist-group-forum-messages.html>
3. <http://ddanchev.blogspot.com/2006/05/terrorist-social-network-analysis.html>
4. <http://www.cosc.georgetown.edu/~denning/>
5. <http://idefense.com/methodology/>
6. <http://www.cert.org/archive/html/spie.html>
7. [http://counterterrorismblog.org/2006/06/internet\\_security\\_team\\_finds\\_j.php](http://counterterrorismblog.org/2006/06/internet_security_team_finds_j.php)
8. [http://tajdeed-list.net/pipermail/pir\\_tajdeed-list.net/2006-June/000092.html](http://tajdeed-list.net/pipermail/pir_tajdeed-list.net/2006-June/000092.html)
9. <http://cryptome.org/>
10. <http://ddanchev.blogspot.com/2006/05/current-emerging-and-future-state-of.html>
11. <http://ddanchev.blogspot.com/2006/02/hacktivism-tensions.html>
12. <http://www.jpost.com/servlet/Satellite?cid=1150885871095&pagename=JPost%2FJPArticle%2FShowFull>

13. <http://del.icio.us/DDanchev/Terrorism>
14. <http://del.icio.us/DDanchev/Cyberterrorism>
15. <http://www.usip.org/pubs/specialreports/sr116.html>
16. [http://www.adl.org/internet/jihad\\_online.pdf](http://www.adl.org/internet/jihad_online.pdf)
17. <http://www.inach.net/content/Annual%20Report%20jugendschutz.pdf>
18. <http://siteinstitute.org/websites.html>
19. <http://siteinstitute.org/>
20. <http://www.bcpl.net/~rfrankli/hatedir.htm>
21. <http://www.bcpl.net/~rfrankli/hatedir.pdf>
22. [http://firstmonday.org/issues/issue6\\_2/ray/index.html](http://firstmonday.org/issues/issue6_2/ray/index.html)

386

### **North Korea - Turn On the Lights, Please (2006-06-29 03:56)**

[1]North Korea's recent missile launch furor, and the obvious conventional weaponry doctrine in place, as well as my

comments in the [2]Travel Without Moving series - Korean Demilitarized Zone, reminded me of a how they tend to

fuel growth in military spending/[3]the regime, where the trade-off is a developing economy, or any economy at all.

I feel [4]North Korea is still quite dark these days, very impressive imagery showing that :

*" South Korea is bright, North Korea is dark. This amazing image is included in the standard US Department of*

*Defense briefings on North Korea. It was mentioned in a [5] news briefing on 23 December 2002 by Defense Secretary Rumsfeld, who stated that "If you look at a picture from the sky of the Korean Peninsula at night, South Korea is filled with lights and energy and vitality and a booming economy; North Korea is dark." There are a number of versions of this image in circulation, with visible differences that vary according to the conditions at the time the imagery was acquired. "*

Rich Karlgaard's comment on [6]lifting North Korea sanctions, and Quentin Hardy's argument that *" Capitalism has corrupted other authoritarian regimes, why not North Korea? "*are worth taking into consideration.

1. <http://cryptome.org/dprk-furor/dprk-eyeball.htm>
2. [http://ddanchev.blogspot.com/2006/05/travel-without-moving-korean\\_27.html](http://ddanchev.blogspot.com/2006/05/travel-without-moving-korean_27.html)
3. <http://www.hrnk.org/hiddengulag/toc.html>
4. <http://www.globalsecurity.org/military/world/dprk/dprk-dark.htm>
5. <http://www.globalsecurity.org/military/library/news/2002/12/mil-021223-usia01.htm>

6.

[http://blogs.forbes.com/digitalrules/2006/06/should\\_we\\_lift\\_.html](http://blogs.forbes.com/digitalrules/2006/06/should_we_lift_.html)

387

## **The WarDriving Police and Pringles Hacking (2006-06-30 03:52)**

These days you never know where the next hacking attempt on your wireless network may come from. In this case,

it's from the police, as [1]authorities start mimicking wardriving behavior :

*" The Douglas Country Sheriff's DOffice says it's going to start warning computer users that their networks may be vulnerable to hackers. The Sheriff's Department plans to equip several of its community service and patrol cars*

*with devices that detect unprotected computer networks. In cases where investigators can figure out who owns the*

*networks, they'll try to warn of potential security issues. They'll also drop off brochures with instructions to computer users on how to password protect their networks. "*

Back in 2004, Kelly Martin wrote a very pragmatic article on [2]Catching a virus writer, emphasizing on how

*" with the consumer WiFi explosion, launching a virus into the wild has never been easier and more anonymous than it is today. "* Moreover, Kaspersky labs recently assessed the [3]situation in England, and you can easily see the need of basic awareness there.

I don't feel it's a good idea mainly because it generates more noise for the end user to sort through. They'd

rather assess and position on a map the regions with most vulnerable networks and figure out a cost-effective ways

of spreading awareness in these regions, instead of taking the role of an ethical wardriving. On the other hand,

if they start taking care of wireless, would they start [4]taking into consideration [5]Bluetooth as well? There're

just too many ethical wardrivers to deal with and [6]deceive these days, and creative end users tend to [7]multiply

themselves or, of course, use common sense protection.

WarDriving Awareness brochure courtesy of [8]Tom Hayward.

Recommended reading - "[9]War, Peace, or

Stalemate: Wargames, Wardialing, Wardriving, and the Emerging Market for Hacker Ethics".

1.

[\[D=0c76dce6-ac1f-02d8-0047-c589c01ca7bf\]\(http://www.9news.com/acm\_news.aspx?OSGNAME=KUSA&IKOBJECTID=1db245df-0abe-421a-019d-d112657c4feb&TEMPLATEI\)](http://www.9news.com/acm_news.aspx?OSGNAME=KUSA&IKOBJECTID=1db245df-0abe-421a-019d-d112657c4feb&TEMPLATEI</a></p></div><div data-bbox=)

2. <http://www.securityfocus.com/columnists/246>

3. <http://www.viruslist.com/en/analysis?pubid=187008611>

4.

[http://trifinite.org/Downloads/21c3\\_Bluetooth\\_Hacking.pdf](http://trifinite.org/Downloads/21c3_Bluetooth_Hacking.pdf)

5. <http://www.viruslist.com/en/analysis?pubid=188833782>
6. <http://www.remote-exploit.org/index.php/Hotspotter>
7. <http://packetstorm.linuxsecurity.com/wireless/fakeap-0.2.tar.gz>
8. <http://www.tomh.us/>
9. [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=585867](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=585867)

388

### **Real-Time PC Zombie Statistics (2006-06-30 04:56)**

Zombies inevitably turning into [1]botnets represent a huge, automated and efficient advantage to [2]malicious

attackers, I topic and most of its dimensions I covered in my [3]Future trends of malware research. [4]CipherTrust's

Zombie Stats help you measure the approximate population of infected zombie PCs according to the vendor's [5]Trust-

edSource. Not surprisingly, China's steadily increasing novice Internet population, both represents a growing menace

to the entire Internet, and a market development opportunity for AV and security vendors. The situation is getting

of hand with ISPs upgrading Internet connections, while still not putting enough efforts when it comes to dealing

with botnets. And while some are [6]taking actions under enforcement, major [7]ISPs are still reluctant to face the

issue – ISPs still prefer to offer security services on a license basis or through reseller partnerships, though I’m certain there’s an entire market segment waiting to be discovered by them if they manage to reset their position in this space.

Moreover, [8]Prolexic’s Zombie report for Q1-Q2 2005, provides even more detailed info, and a neat [9]visual-

ization of the routes involved with DDoS attacks, where the blue represents the U.S, and the red China. For the the

time being, the [10]ShadowServer guys keep on enthusiastically dealing with the problem, for no profit at all.

1. <http://ddanchev.blogspot.com/2006/02/war-against-botnets-and-ddos-attacks.html>

2. <http://ddanchev.blogspot.com/2006/01/what-are-botnet-herds-up-to.html>

3. <http://www.packetstormsecurity.org/papers/general/malware-trends.pdf>

4. <http://www.ciphertrust.com/resources/statistics/zombie.php>

5. <http://www.trustedsource.org/>

6. [http://news.com.com/Australian+ISPs+tapped+to+kill+zombies/2100-7348\\_3-5938170.html](http://news.com.com/Australian+ISPs+tapped+to+kill+zombies/2100-7348_3-5938170.html)

7. [http://www.zdnet.com.au/news/security/soa/ISPs\\_accused\\_of\\_ignoring\\_botnet\\_invasion/0,2000061744,39257307,](http://www.zdnet.com.au/news/security/soa/ISPs_accused_of_ignoring_botnet_invasion/0,2000061744,39257307,)

[00.htm](#)

8. <http://www.prolexic.com/zr/>

9. <http://ddanchev.blogspot.com/2006/03/visualization-in-security-and-new.html>

10. <http://www.shadowserver.org/>

389

**2.7**

**July**

390

## **Hacktivism Tensions - Israel vs Palestine Cyberwars (2006-07-01 17:18)**

Oops, they [1]did it again. The most recent case of [2]hacktivism recently occurred :

*" Shortly after IDF tanks rolled into Gaza, another old front of conflict was reopened early Wednesday morning, but in this battle Kassam rockets and artillery shells were replaced by worms and viruses as pro-Palestinian hackers shut down approximately 700 Israeli web domains. A range of different Web sites were targeted by the group,*

*including Web sites of banks, medical centers, car manufacturers and pension funds. Well-known companies and*

*organizations, including **Bank Hapoalim**, the **Rambam Medical Center**, **Bank Otsar Ha-Hayal**, **BMW Israel**, **Subaru***



***Israel and Citr en Israel, real estate company Tarbut-Hadiur and the Jump fashion Web site all found their Web sites shut down and replaced by the message: Hacked by Team-Evil Arab hackers u KILL palestin people we KILL Israel servers. "***

[3]Zone-H has naturally covered the event and mirrored it, in between receiving an official PR release from the

defacement group – guess it's not just [4]terrorists with cheap marketing teams given the badly structured press

release. What these folks don't seem to be able to realize is that if they were to deface every web site hosting the

infamous [5]Muhammad cartoons, they would end up with a full-time job doing so. What's worth mentioning is

the nature of defaced servers, banks, hospitals, private sector companies, my point is that if they were really up to

causing havoc, they had the necessary privileges to do so. Let's not think on loud on worst case "what if" analysis though.

[6]Defacements are a great example of [7]PSYOPS , most importantly the indirect way of undermining a coun-

try's population confidence in their abilities to win any war or political campaign. During WWII brochures were laying

around everywhere, and planes were dropping them across various cities to, either undermine, or influence the

opinion of the locals towards their vision. The power of the Internet echo is what they're aiming to achieve, and

while I may be whispering their "achievements" even further, the visitors of the affected sites partly got exposed to their propaganda. It's also to interesting to think of PSYOPS in reverse, that is [8]users in countries with restrictive regimes trying to reach out the rest of world through malware – [9]beneficial [10]malware, or beneficial PSYOPS?

What the current, emerging and future state of Hacktivism? In her outstanding research titled "[11]Hacktivism and

the Future of Political Participation", Alexandra Samuel points out some of the key points to keep in mind, and

constructively speculates on the future trends.

At the bottom line, what's all the fuss about? No, it's not because an Israeli covert operative was kidnapped

and held hostage, but because of an 18 years old "[12]destruction machine" which reminds me of the way we used to argue and wage wars on the sand around the same age. The type of, "the wind has just blown your soldier way

beyond the DMZ, and therefore we have no other choice but to attack you with all our forces. Resistance is futile!"

conflicts.

Go to school, hell, even go to an ethical hacking one, or else you'll end up like a walking sausage having to

squeeze yourself with a belt so tight in order not to have your pants fall down! Automated defacement tool shot

courtesy of [13]WebSense. And btw, how was your **[14]July Morning?**

## **Related resouces :**

[15]Israeli-Palestinian Cyberconflict (IPCC) - the complete coverage back in 2001!

[16]The Israeli-Palestinian Cyberconflict

[17]Activism, Hacktivism, and Cyberterrorism : The Internet as a Tool for Influencing Foreign Policy

[18]The Cycle of Cyber Conflict

391

[19]Cyber Attacks During the War on Terrorism

[20]Examining the Cyber Capabilities of Islamic Terrorist Groups

[21]Cyberprotests : The Threat to the U.S Information Infrastructure

[22]Analysis: U.S.-China 'cyberwar' fires blanks

[23]Techno Imperialism and the Effect of Cyberterrorism

[24]Cyberterrorism - don't stereotype and it's there!

[25]Cyberterrorism - recent developments

1. <http://www.jpost.com/servlet/Satellite?cid=1150885871095&pagename=JPost%2FJPArticle%2FShowFull>

2. <http://photos1.blogger.com/blogger/1933/1779/1600/hacktivism.jpg>

3. <http://www.zone-h.org/content/view/13791/30/>
4. <http://ddanchev.blogspot.com/2006/06/tracking-down-internet-terrorist.html>
5. <http://cryptome.org/muhammad.htm>
6. [http://www.zone-h.org/component/option,com\\_topatt/Itemid,49/](http://www.zone-h.org/component/option,com_topatt/Itemid,49/)
7. [http://en.wikipedia.org/wiki/Psychological\\_operations](http://en.wikipedia.org/wiki/Psychological_operations)
8. <http://www.ravantivirus.com/virus/showvirus.php?v=216>
9. <http://www.securityfocus.com/news/11373>
10. <http://www.people.frisk-software.com/~bontchev/papers/goodvir.html>
11. <http://www.alexandrasamuel.com/20060510/now-available-hacktivism-the-future-of-political-participation>
12. <http://en.wikipedia.org/wiki/Rambo>
13. <http://www.websense.com/securitylabs/blog/>
14. [http://www.lyricsfreak.com/u/uriah+heep/july+morning\\_20142398.html](http://www.lyricsfreak.com/u/uriah+heep/july+morning_20142398.html)
15. [http://www.securitymanagement.com/library/Israeli\\_pales0401.pdf](http://www.securitymanagement.com/library/Israeli_pales0401.pdf)
16. [http://www.soc.utu.fi/polhist/vaihtuvat/jokisipila\\_Interfada.pdf](http://www.soc.utu.fi/polhist/vaihtuvat/jokisipila_Interfada.pdf)

17. [http://www.rand.org/pubs/monograph\\_reports/MR1382/MR1382.ch8.pdf](http://www.rand.org/pubs/monograph_reports/MR1382/MR1382.ch8.pdf)
18. <http://militaryreview.army.mil/download/English/MarApr03/alen.pdf>
19. [http://www.ists.dartmouth.edu/analysis/cyber\\_a1.pdf](http://www.ists.dartmouth.edu/analysis/cyber_a1.pdf)
20. <http://www.ists.dartmouth.edu/library/164.pdf>
21. <http://www.au.af.mil/au/awc/awcgate/nipc/cyberprotests.pdf>
22. <http://archives.cnn.com/2001/TECH/internet/05/11/china.cyberwar.idg/index.html>
23. <http://ddanchev.blogspot.com/2006/05/techno-imperialism-and-effect-of.html>
24. <http://ddanchev.blogspot.com/2005/12/cyberterrorism-dont-stereotype-and-its.html>
25. <http://ddanchev.blogspot.com/2006/01/cyberterrorism-recent-developments.html>

392

### **China's Interest of Censoring Mobile Communications (2006-07-02 02:53)**

Just came across to a great article at the IHT on [1]China's interest of tightening control of cellphones :

*" The new measures being contemplated for tightening control of cellphone use reportedly include mandatory*

*user registration. Users now can easily buy cellphone cards at any convenience store, instantly obtaining a new*

*phone number without identifying themselves. Whether through speech or short messaging, cellphones have played*

*a major role in a wave of social unrest that has swept China in the last two years, allowing people to organize quickly and to spread news of police actions and other developments. Anonymous use of cellphones is a major loophole at*

*a time when the state is investing heavily on monitoring communications of all kinds, and the authorities appear determined to close it"*

Whereas there's been quite some media coverage on China's Internet censorship efforts, the country's under-

developed income distribution model results in more people having access to plain simple cellphone communications

compared to owning a PC. And even if they own a PC, or use public ones to access the Internet, information from

China's provinces where the real China is, often breaks out through SMS messages – or [2]comes in. Venus Info

Tech's [3]**Cybervision SMS Filtering System** is what they've been using, and it seems it's the government's long-term partner. The article also points out on the illegality of reporting or broadcasting information on "sudden events", consider the [4]SARS virus as one of these. Yet another in-depth article, indicates the only [5]usefulness out of this

copyright, or let's use a more friendly term, such as content monitoring/filtering, which is the detection of banking

frauds and other scams – can you censor "[6]Bware, SMS und Ctrl" or learn to encode in such a way?

From a business perspective, the [7]Chinese Internet population represents a hot opportunity for companies

offering censorship-circumvention services – [8]IP cloaking and competitive intelligence among the other needs. It's

interesting to note U.S government's interest in Chinese citizens having access to more information :

*" Ultrareach and Dynamic Internet Technology (DIT) in North Carolina, both connected to Falun Gong, receive*

*U.S. government funding through the International Broadcasting Bureau to help it get Voice of America and Radio*

*Free Asia to Chinese Web surfers. Each day, DIT sends out millions of emails and text messages containing proxy links to Chinese citizens. About one million users have downloaded DIT's circumvention software, which automatically*

*links to the firm's proxy servers, while "hundreds of thousands" directly access the proxy Web sites daily, said founder Bill Xia. UltraReach, claims 100,000 users use its proxies. All told, the IBB spends about \$5 million a year on contracts with hacktivists and firms on censorship-busting efforts in countries such as China and Iran. "*

I also came across to an informative research on the topic, "[9]The Wireless Leash : Mobile Messaging Service

as a Means of Control". Recommended reading in case you want to know more on the topic from a social and

political perspective, as well as go through many relevant cases.

**UPDATE :** [10]China restricts Internet cafe access - "*Rules on children in Internet cafes were imposed after Chinese officials warned that students were spending too much time playing online games and were getting access to violent and obscene material.*"

### **Related resources:**

[11]Censorship

[12]China

[13]2006 = 1984?

[14]Anonymity or Privacy on the Internet?

[15]World's Internet Censorship Map

[16]China - the biggest black spot on the Internet's map

[17]Chinese Internet Censorship efforts and the outbreak

393

[18]Securing political investments through censorship

1. <http://www.iht.com/articles/2006/06/30/news/china.php>

2. [http://www.usatoday.com/tech/news/2005-06-30-politics-text-tool\\_x.htm?csp=34](http://www.usatoday.com/tech/news/2005-06-30-politics-text-tool_x.htm?csp=34)



3. [http://www.venusense.com/html/product/product\\_08.htm](http://www.venusense.com/html/product/product_08.htm)
4. <http://www.theepochtimes.com/news/4-7-12/22391.html>
5. <http://www.bloomberg.com/apps/news?pid=10000080&sid=aE87osXqUmRw&refer=asia>
6. [http://www.rsf.org/article.php3?id\\_article=10870](http://www.rsf.org/article.php3?id_article=10870)
7. <http://www.mercurynews.com/mld/mercurynews/14948550.htm>
8. <http://ddanchev.blogspot.com/2005/12/ip-cloaking-and-competitive.html>
9. [http://ihome.cuhk.edu.hk/~b200167/files/giu\\_wireless\\_leash.pdf](http://ihome.cuhk.edu.hk/~b200167/files/giu_wireless_leash.pdf)
10. [http://news.yahoo.com/s/ap/20060703/ap\\_on\\_hi\\_te/china\\_in\\_ternet\\_crackdown](http://news.yahoo.com/s/ap/20060703/ap_on_hi_te/china_in_ternet_crackdown)
11. <http://del.icio.us/DDanchev/Censorship>
12. <http://del.icio.us/DDanchev/China>
13. <http://ddanchev.blogspot.com/2006/01/2006-1984.html>
14. <http://ddanchev.blogspot.com/2006/01/anonymity-or-privacy-on-internet.html>
15. <http://ddanchev.blogspot.com/2006/06/worlds-internet-censorship-map.html>
16. <http://ddanchev.blogspot.com/2006/01/china-biggest-black-spot-on-internets.html>

17. <http://ddanchev.blogspot.com/2006/02/chinese-internet-censorship-efforts.html>

18. <http://ddanchev.blogspot.com/2006/04/securing-political-investments-through.html>

394

### **BBC under the Intelligence Shadow (2006-07-03 00:57)**

Nothing is impossible, the impossible just takes a little while. A relatively typical practices for the ex-USSR, namely

controlling the media and profiling the journalists including the readers, seem to have been going on in London

during the same period as well. According to the Sunday Telegraph, the [1]BBC let intelligence agents vet staff :

*" Confidential papers obtained by the Sunday Telegraph reveal that the British Broadcasting Corp. allowed in-*

*telligence agents to investigate the backgrounds and political affiliations of thousands of its employees, including newsreaders, reporters and continuity announcers. The files, which shed light on the BBC's hitherto secret links with the counter-espionage service known as MI5, show that at one stage it was responsible for vetting 6,300 BBC posts*

*- almost a third of the total work force. The procedure was phased out in the late 1980s. The files also show that*

*the corporation maintained a list of "subversive organizations" and that evidence of certain kinds of political activity could be a bar to appointment or promotion. "*

If you can spell the name of the party while sleeping, and have subscribed to its periodical propaganda, only

then you have the chance to unleash your career potential. I guess what they were worried about was an undercover

Red reporter , taking advantage of live events and directly broadcasting a subvertive message – remember when

a guy invaded Truman's world in the "Truman show", and tried to warn the little kid he's on TV all the time? The interesting part is how even the spouses of applicants were subject to scrutiny.

There you go with the freedom of the press, I guess China must have had something in mind when blocking

access to the BBC's web site.

1. <http://washingtontimes.com/world/20060701-105304-4152r.htm>

395

### **How to Win the U.S Elections (2006-07-05 14:51)**

Juicy barbecues, hugging babies, in between offering, and asking for the Moon days are over. E-voting is the future

of technological political engineering. So, how can you win the U.S Elections?

**01.** Ensure one company holds a virtual monopoly in E-voting systems, thus contributing to yet another monocultural insecurity. If it naturally has some competition, insist its systems are placed in key regions, where barbecues wouldn't work.

**02.** Start a nation-wide PR campaign emphasizing on the benefits of E-voting. Mention it's innovative, it's go-

ing to cut costs while providing you with flexibility, the way it provides flexibility to citizens abroad, moreover, also

emphasize on the increased speed of the results.

**03.** Make sure the rural areas where the masses of technologically unsophisticated citizens are the ones tak-

ing advantage of this immature concept. The point is that, even if there's an error, they got no chance of defining it.

**04.** If something "goes wrong" forward all the responsibility to the virtual monopolist, and promise precautions against future possibilities for modifying the results - anyway, sorry folks the elections are over, so till next time keep on speculating what actually happened.

Meanwhile, on the other side of the universe, where we should perhaps thank Jesus for coming up with

more colours in live, than black and white only, I stumbled upon an [1]Unredacted Diebold Black Box Voting Hack

Reports with quite some disturbing images. Make sure the efficacy that you wish for, doesn't actually happen. A

friend also tipped me on this quite [2]longish report on the topic, and didn't forget to warn me to remove my 3D

glasses before reading it either.

**UPDATE :** [3]Interesting political reading related to veto power.

Clippy votes courtesy of the [4]EFF.

1. <http://cryptome.org/bbv070306.htm>
2. <http://www.brennancenter.org/programs/downloads/Full%20Report.pdf>
3. <http://www.cnn.com/2004/ALLPOLITICS/01/07/elec04.prez.bush.no.vetoes.ap/>
4. <http://www.eff.org/Activism/E-voting/>

396

### **Travel Without Moving - North Korea Missile Launch Pad (2006-07-06 03:03)**

Seems like it's North Korea's most active PR month given the [1]public outbreak due to their unsuccessful launch of an intercontinental missile, so in these Travel Without Moving series I decided to feature the launch pad, originally came across it, nowhere else but at [2]Cryptome's well sorted photo gallery of the event. Whereas the U.S is activating diplomatic ties in order to put more pressure on North Korea's tests, [3]China and Russia among the rest of the superpowers seems to be teasing the U.S in a way only they can afford to - let's don't forget the financial incentives for [4]Russia to enrich Iran's uranium altogether. As far as Kim Jong Il is concerned, in between fueling growth in the [5]infrastructure necessary to maintain a regime, he [6]enjoys making [7]secret meetings with ex-comrades while

travelling to Moscow with his armoured train, as he's afraid of flying.

**Previous series, related posts :**

[8]Travel Without Moving - Typhoon Class Submarines

[9]Travel Without Moving - Cheyenne Mountain Operations Center

[10]Travel Without Moving - KGB Lubyanka Headquarters

[11]Travel Without Moving - Korean Demilitarized Zone

[12]Travel Without Moving - Georgi Markov's KGB Assassination Spot

[13]Travel Without Moving - Scratching the Floor

[14]North Korea - Turn On the Lights, Please

[15]Who Needs Nuclear Weapons Anymore?

[16]Who's Who in Cyber Warfare?

[17]Is a Space Warfare Arms Race Really Coming?

[18]EMP Attacks - Electronic Domination in Reverse

1. <http://www.voanews.com/english/2006-07-05-voa22.cfm>

2. <http://cryptome.org/dprk-furor/dprk-eyeball.htm>

3. [http://news.yahoo.com/s/ap/20060705/ap\\_on\\_re\\_as/un\\_north\\_korea\\_10;\\_ylt=AmpEO5lYL\\_Q0CDvjF0d6VviCscEA;\\_ylu=X3](http://news.yahoo.com/s/ap/20060705/ap_on_re_as/un_north_korea_10;_ylt=AmpEO5lYL_Q0CDvjF0d6VviCscEA;_ylu=X3)

[oDMTBiMW04NW9mBHNIYwMIJVRPUCUI](#)

4.

<http://www.smh.com.au/news/world/iran-russia-reach-agreement-to-enrich-uranium/2006/02/27/1140888771985.html>

5. <http://www.hrnk.org/hiddengulag/toc.html>

6. <http://news.bbc.co.uk/2/hi/europe/1476466.stm>

7.

[http://english.ohmynews.com/ArticleView/article\\_view.asp?menu=A11100&no=301166&rel\\_no=1&back\\_url=](http://english.ohmynews.com/ArticleView/article_view.asp?menu=A11100&no=301166&rel_no=1&back_url=)

8. <http://ddanchev.blogspot.com/2006/05/travel-without-moving-typhoon-class.html>

9. <http://ddanchev.blogspot.com/2006/05/travel-without-moving-cheyenne.html>

10. <http://ddanchev.blogspot.com/2006/06/travel-without-moving-kgb-lubyanka.html>

11. [http://ddanchev.blogspot.com/2006/05/travel-without-moving-korean\\_27.html](http://ddanchev.blogspot.com/2006/05/travel-without-moving-korean_27.html)

12. <http://ddanchev.blogspot.com/2006/06/travel-without-moving-georgi-markovs.html>

13. <http://ddanchev.blogspot.com/2006/05/travel-without-moving-scratching-floor.html>

14. <http://ddanchev.blogspot.com/2006/06/north-korea-turn-on-lights-please.html>

15. <http://ddanchev.blogspot.com/2006/02/who-needs-nuclear-weapons-anymore.html>
16. <http://ddanchev.blogspot.com/2006/05/whos-who-in-cyber-warfare.html>
17. <http://ddanchev.blogspot.com/2006/03/is-space-warfare-arms-race-really.html>
18. <http://ddanchev.blogspot.com/2006/05/emp-attacks-electronic-domination-in.html>

397

### **\$960M and the FBI's Art of Branding Insecurity (2006-07-06 10:31)**

In previous posts "[1]Are cyber criminals or bureaucrats the industry's top performer?", and "[2]Insiders - insights, trends and possible solutions" I emphasized on how bureaucracy results in major insecurities, and provided further

info on various issues related to insiders and [3]risk [4]management [5]solutions - ones the FBI is obviously far from implementing given the access control issues they have in place. It seems like two years ago, a [6]Consultant

Breached FBI's Computers :

*" A government consultant, using computer programs easily found on the Internet, managed to crack the FBI's*

*classified computer system and gain the passwords of 38,000 employees, including that of FBI Director Robert S.*

*Mueller III. The break-ins, which occurred four times in 2004, **gave the consultant access to records in the Witness***



***Protection Program and details on counterespionage activity***, according to documents filed in U.S. District Court in Washington. As a direct result, the bureau said it was forced to temporarily shut down its network and commit

*thousands of man-hours and millions of dollars to ensure no sensitive information was lost or misused. "*

How he did it? With access to hashes and 90 days password expiration period, he had all the time in the

world, excluding the fact that according to the article a FBI agent even gave him his password.

[7]Passwords are a hot topic, and so are the [8]insecurities posed by them. Moreover, spending near \$1B for

a non-existent case system, while dealing with access control issues is rather unserious for thought to be serious

institution – have you guys considered an open source alternative? You wouldn't come across lots of developers with

top-secret clearances applying for the top, but obviously a top-secret clearance cannot prevent [9]insider behavior

as well.

1. <http://ddanchev.blogspot.com/2006/03/are-cyber-criminals-or-bureaucrats.html>

2. <http://ddanchev.blogspot.com/2005/12/insiders-insights-trends-and-possible.html>

3. <http://www.vontu.com/>

4. <http://www.reconnex.net/>

5. <http://www.tablus.com/>
6. [http://www.washingtonpost.com/wp-dyn/content/article/2006/07/05/AR2006070501489\\_pf.html](http://www.washingtonpost.com/wp-dyn/content/article/2006/07/05/AR2006070501489_pf.html)
7. <http://ddanchev.blogspot.com/2006/02/end-of-passwords-for-sure-but-when.html>
8. <http://ddanchev.blogspot.com/2005/12/how-to-create-better-passwords-why.html>
9. <http://ddanchev.blogspot.com/2005/12/insiders-insights-trends-and-possible.html>

398

## **Delicious Information Warfare - 27/07 (2006-07-08 01:25)**

Given the interest in the perspective, I'm continuing to share my daily reads for the last week and a half. Catch up

with [1]previous [2]summaries, and see [3]the big picture as well.

**01. [4]The fine art of shoulder surfing** - Many hackers download their tools but traditionalists skilled in shoulder surfing still pose a threat. to [5]Security **on july 2**

**02. [6]VCs discuss the next big things** - Cell phone gambling in China and other wireless trends are what venture capitalists at Brainstorm were talking about. to [7]Investing [8]Mobile **on july 2**

**03. [9]Life After Privacy** - Personal information is no longer personal. The only question is: who gets to see it? to [10]Security [11]Privacy **on july 2**

#### **04. [12]Spy Agency Sought U.S. Call Records Before 9/11, Lawyers Say - The U.S. National Security Agency**

asked AT &T Inc. to help it set up a domestic call monitoring site seven months before the Sept. 11, 2001 attacks,

lawyers claimed June 23 in court papers filed in New York federal court. to [13]Intelligence [14]Surveillance [15]Wire-

tapping [16]Terrorism [17]NSA **on july 2**

#### **05. [18]MySpace, a place without MyParents - Scott Granneman looks at the mass hysteria surrounding MyS-**

pace social security issues, examines a collection of frightening reports, and then discusses the real issue of parenting and parental supervision behind keeping our children safe. to [19]Security [20]NewMedia [21]MySpace

**on july 2**

#### **06.**

#### **[22]Limiting Vulnerability Exposure through effective Patch Management: threat mitigation through**

**vulnerability remediation** - This document aims to provide a complete discussion on vulnerability and patch

management. It looks first at the trends relating to vulnerabilities, exploits, attacks and patches. These trends

provide the drivers of patch and vulnerability management. to [23]Vulnerabilities [24]0day **on july 2**

#### **07. [25]'Blue Pill' Prototype Creates 100 % Undetectable Malware - Joanna Rutkowska, a stealth malware re-**

searcher at Singapore-based IT security firm COSEINC, says the new Blue Pill concept uses AMD's SVM/Pacifica

virtualization technology to create an ultra-thin hypervisor that takes complete control of the underlying.. to

[26]Malware [27]Rootkit [28]Technology **on july 2**

**08. [29]Hacker attacks hitting Pentagon -** "This stuff is enormously important," said John P. Stenbit, the Pentagon's chief information officer until 2004. "If the keys get into the wrong hands, all kinds of bad things happen. to

[30]Defense [31]InformationWarfare **on july 2**

**09. [32]Data Mining Myspace Bulletins -** I was able to whip together a small C program that generates urls, retrieves the bulletin, and saves the html to a file. Once all of the data has been downloaded, it's easy to parse

through using a tool like grep. to [33]Security [34]NewMedia [35]MySpace **on july 2**

**10. [36]How A Trigger Set Off A Logic Bomb At UBS PaineWebber -** A forensics investigator testifying at the computer sabotage trial of a former systems administrator for UBS PaineWebber detailed how each line of code in

the trigger helped set off a devastating logic bomb. to [37]Insider [38]Malware **on july 2**

**11. [39]On the Economics of Information Security - Papers -** The Fifth Workshop on the Economics of Infor-

mation Security (WEIS 2006). to [40]Security [41]Leadership **on july 2**

**12. [42]What's Wrong with This Picture? -** A messy desk is a vulnerable desk. We've created one with 20

egregious violations of a good policy. See if you can find them. to [43]Security [44]Workplace **on july 2**

399

**13. [45]Space attack on satellites could be devastating -** If the US does not protect its Earth-orbiting satellites, the equivalent of a car bomb in space could take the economy back to the 1950s, according to witnesses

testifying in Washington DC earlier this week. to [46]Military [47]Satellite [48]Space [49]SPAWAR **on july 2**

**14. [50]Air Force to spend \$450K datamining blogs for war on terror -** The Air Force Office of Scientific Research recently began funding a new research area that includes a study of blogs. Blog research may provide

information analysts and warfighters with invaluable help in fighting the war on terrorism. to [51]Intelligence

[52]Terrorism [53]Surveillance [54]Technology **on july 2**

**15. [55]How Did U.S. Assess Iraqi Bioweapon Production? -** One of the most vivid allegations made by the

U.S. government regarding Iraqi weapons of mass destruction was the claim that Iraq had developed mobile

laboratories for the production of biological weapons. to [56]Intelligence **on july 2**

**16. [57]Month of Browser Bugs** - I will publish one new vulnerability each day during the month of July as

part of the Month of Browser Bugs project. to [58]Vulnerabilities [59]0day [60]Metasploit **on july 3**

**17. [61]IM's Hidden Dangers** - But unlike water-cooler chatter, IMs leave a trail—one that can be tracked by employers, regulators, and law-enforcement officials. And like e-mail, IMs are considered legal documents. to [62]IM

[63]Compliance **on july 6**

**18. [64]Trend Micro Execs Face Probe** - Agency may charge CEO and her husband with trading in shares of

his former company, SINA. Trend Micro reported revenues of \$621.9 million in 2005, compared with \$587.4 million

in 2004. The company currently has nearly 3,000 employees around the world. to [65]Investing [66]AntiVirus **on july 6**

**19. [67]Blast from the past: '50s Nevada A-bombs light LA's night sky** - In the early 1950s, several above-

ground atom bomb tests at the Nevada Proving Ground were visible in Los Angeles. This photo and five similar ones

from 1951-1955 are from the Los Angeles Public Library Photo Database. to [68]Defense [69]Nuclear [70]Technology

**on july 6**

**20. [71]FOIA at Forty** - The fortieth anniversary of the Freedom of Information Act, signed into law by President Johnson on July 4, 1966, was marked with the release of several interesting and informative publications.

to [72]FOIA **on july 6**

**21. [73]Early Days On The Anti-Virus Front: A Personal Perspective** - An anti-virus programmer reminisces

about the people and the organizations that were pivotal in the earliest days of the war against computer viruses.

to [74]Malware [75]AntiVirus **on july 6**

**22. [76]The Blue Pill Hype** - The working prototype I have (and which I will be demonstrating at SyScan and Black Hat) implements the most important step towards creating such malware, namely it allows to move the

underlying operating system, on the fly, into a secure virtual machine. to [77]Malware [78]Rootkit [79]Innovation **on**

**july 6**

**23. [80]New PoC virus can infect both Windows and Linux** - The virus is interesting, said analysts on Kaspesky's Viruslist website, because it is capable of infecting ELF, the file format used for Linux systems, and PE, Windows' file format. to [81]Malware **on july 6**

**24. [82]Iranian intelligence services ban access to Azerbaijani websites** - He reported that the ban aims at depriving Iranian Azerbaijanis of the contact with the international community. to [83]Censorship [84]Intelligence

[85]Iran **on july 6**

**25. [86]Can the N.Y. Times Be Charged Under the Espionage Act?** - Can The New York Times be prosecuted for their story about the government's secret terrorist finance tracking program? to [87]Intelligence [88]Espionage [89]Terrorism [90]FreeSpeech **on july 6**

**26. [91]Text messaging censorship: PITA, BFD, or BTHOM?** - Text messaging and the first level of censorship begins at the phone. While it's certainly possible to enter any word using the alphabetic method in which a=2, b=2-2, c=2-2-2, d=3 and so on, it isn't very convenient. to [92]Censorship [93]Mobile **on july 6**

**27. [94]Iran Accuses Academic Of Espionage For U.S.** - Iran today accused jailed academic Ramin Jahanbegloo of having spied for the United States, with the aim of toppling the ruling Islamic system. to [95]Intelligence [96]Espionage [97]Iran **on july 6**

**28. [98]Italian intelligence officials arrested over CIA kidnap** - Italian police arrested two officials with Italy's military intelligence agency on Wednesday on suspicion of helping the CIA in the alleged kidnapping of a terrorism suspect in Milan, judicial sources said. to [99]Intelligence [100]Espionage [101]CIA **on july 6**

**29. [102]New York Times Draws Criticism Over Decision to Reveal Intelligence Program** - Executive editor of the New York Times Bill Keller and former director of the NSA Admiral Bobby Inman debate the newspaper's



publication of the Bush administration's surveillance of banking records and the process in deciding what is fit to

print. to [103]FreeSpeech **on july 6**

**30. [104]Hackers May Lose Nuclear Option** - The risk was illustrated in 2003, when the Slammer worm pene-

trated a network at the idled Davis-Besse nuclear plant in Ohio, disabling a safety monitoring computer for nearly

five hours. to [105]SCADA [106]Nuclear [107]Cyberterrorism [108]Malware **on july 7**

**31. [109]3 arrested in Coca-Cola trade secret scheme**

- "As the health of our enterprise continues to strengthen and the breadth of our innovation pipeline continues to grow, our ideas and our competitive data carry increasing

interest to those outside our business." to [110]Insider [111]Espionage **on july 7**

**32. [112]Proactive Protection: a Panacea for Viruses?**

- The first in a series of articles that discuss the newest technologies used by antivirus companies which focuses on proactive technologies. to [113]Malware [114]Innovation

**on july 7**

**33. [115]Japan to speed up installation of missile defense system** - The envisioned missile defense system

will detect launches of ballistic missiles with Aegis and other sophisticated radar systems and shoot them down with

the sea-based Standard Missile-3 and the land-based Patriot Advanced Capability-3. to [116]Defense [117]Military

**on july 7**

**34. [118]FCC CALEA Wiretap Rule for Broadband and VOIP** - This document addresses the assistance capabilities required, pursuant to section 103 of the (CALEA- for facilities-based broadband Internet access providers and

providers of interconnected Voice over Internet Protocol (VoIP). to [119]Security [120]Terrorism [121]Intelligence

[122]Wiretapping [123]CALEA [124]VoIP [125]Compliance  
**on july 7**

**35. [126]Tensions Ramping up with North Korea** - "The U.S. was hell bent on espionage over military objects of the DPRK in March when it staged large-scale RSOI and "Foal Eagle" joint military exercises, bringing about the dark cloud of nuclear warfare." to [127]Defense [128]Military [129]Reconnaissance **on july 7**

**36. [130]Over 1,200 Cases of U.S. Aerial Espionage - Translated 2004 News Items** - Involved in the aerial espionage were latest reconnaissance planes of different missions including U-2, RC-135, E-8C, E-3, RC-7B, RC-12, RF-4, P-3 and

EP-3. to [131]Espionage [132]Military [133]Reconnaissance  
**on july 7**

**37. [134]Interview : An Ethical Hacker Protects the World Cup Network** - Dr. Tom Porter is the mastermind behind the security for the World Cup network and a lifetime hacker himself. He shares his thoughts about network security,

hacking and protecting the World Cup network. to  
[135]Security [136]Interview [137]Leadership **on july 7**

**38. [138]Google's Microsoft Syndrome** - Google has fixed a security flaw in its RSS reader that could have allowed hackers to steal users' personal information, but experts warned Thursday that the online giant could increasingly

become a magnet for hackers, displacing Microsoft as the No. 1 target to [139]Vulnerability [140]Google [141]New-Media [142]Web **on july 7**

**39. [143]Hefty bill for online click fraud** - Online advertisers paid more than \$800m last year for fraudulent clicks on their ads and more than a quarter of them have reduced their spending as a result, according to a study by the

Outsell media research firm. to [144]NewMedia [145]Advertising [146]Investing **on july 7**

**40. [147]BitDefender Ships Anti-Rootkit Beta** - The anti-virus vendor, based in Bucharest, Romania, on July 7 lifted the wraps off a new anti-rootkit utility that promises to spot and delete stealthy software programs that are used by malicious hackers to hide malware. to [148]Malware [149]AntiVirus [150]Rootkit [151]Technology **on july 7**

**41. [152]VPN market to hit \$29bn by 2009** - The virtual private network (VPN) services market was worth \$23bn (£12.5bn) in 2005 and is expected to grow another 22 per cent to hit \$29bn (£15.8bn) by 2009, according to an

industry analyst. to [153]Security [154]VPN [155]Investing  
**on july 7**

**42. [156]US managers accused of industrial espionage** - Three former US car industry executives have been accused of selling trade secrets to the Chinese. to [157]Espionage [158]Insider **on july 7**

**43. [159]Mod terror documents found in ditch** - According to the newspaper, it includes phone numbers for the UK's most important military figures, such as the Defence Secretary, Chief of Defence Staff and Director of Special

Force. to [160]Security **on july 7**

**44. [161]Authorities say gangs using Internet** - Some of the country's most notorious street gangs have gotten Web-savvy, showcasing illegal exploits, making threats, and honoring killed and jailed members on digital turf. to

[162]PSYOPS **on july 7**

1. <http://ddanchev.blogspot.com/2006/06/delicious-information-warfare-2427.html>

2. <http://ddanchev.blogspot.com/2006/06/delicious-information-warfare-1324.html>

3. <http://del.icio.us/DDanchev?settagview=cloud>

4. <http://www.itweek.co.uk/itweek/comment/2159476/fine-art-shoulder-surfing>

5. <http://del.icio.us/DDanchev/Security>

6. [http://money.cnn.com/rssclick/2006/06/30/magazines/fortune/brainstorm\\_vc/index.htm?section=money\\_technology](http://money.cnn.com/rssclick/2006/06/30/magazines/fortune/brainstorm_vc/index.htm?section=money_technology)
7. <http://del.icio.us/DDanchev/Investing>
8. <http://del.icio.us/DDanchev/Mobile>
9. <http://www.redherring.com/article.aspx?a=17383>
10. <http://del.icio.us/DDanchev/Security>
11. <http://del.icio.us/DDanchev/Privacy>
12. <http://www.bloomberg.com/apps/news?pid=20601087&sid=abIV0cO64zJE&refer=>
13. <http://del.icio.us/DDanchev/Intelligence>
14. <http://del.icio.us/DDanchev/Surveillance>
15. <http://del.icio.us/DDanchev/Wiretapping>
16. <http://del.icio.us/DDanchev/Terrorism>
17. <http://del.icio.us/DDanchev/NSA>
18. <http://www.securityfocus.com/columnists/408>
19. <http://del.icio.us/DDanchev/Security>
20. <http://del.icio.us/DDanchev/NewMedia>
21. <http://del.icio.us/DDanchev/MySpace>
22. <http://singe.rucus.net/masters/thesis/Dominic%20White%20-%20MSc%20-%20Patch%20Management.pdf>

23. <http://del.icio.us/DDanchev/Vulnerabilities>
24. <http://del.icio.us/DDanchev/0day>
25. <http://www.eweek.com/article2/0,1895,1983037,00.asp>
26. <http://del.icio.us/DDanchev/Malware>
27. <http://del.icio.us/DDanchev/Rootkit>
- 402
28. <http://del.icio.us/DDanchev/Technology>
29. <http://www.baltimoresun.com/news/nationworld/balte.nsa02jul02,0,754404.story?coll=bal-home-headlines>
30. <http://del.icio.us/DDanchev/Defense>
31. <http://del.icio.us/DDanchev/InformationWarfare>
32. <http://lists.grok.org.uk/pipermail/full-disclosure/2006-June/047579.html>
33. <http://del.icio.us/DDanchev/Security>
34. <http://del.icio.us/DDanchev/NewMedia>
35. <http://del.icio.us/DDanchev/MySpace>
36. <http://www.informationweek.com/news/showArticle.jhtml?articleID=189601826&subSection=Breaking+News>
37. <http://del.icio.us/DDanchev/Insider>
38. <http://del.icio.us/DDanchev/Malware>

39. <http://weis2006.econinfosec.org/docs/>
40. <http://del.icio.us/DDanchev/Security>
41. <http://del.icio.us/DDanchev/Leadership>
42. <http://www.csoonline.com/read/030104/desk.html>
43. <http://del.icio.us/DDanchev/Security>
44. <http://del.icio.us/DDanchev/Workplace>
45. <http://www.newscientistspace.com/article/dn9393-space-attack-on-satellites-could-be-devastating.html>
46. <http://del.icio.us/DDanchev/Military>
47. <http://del.icio.us/DDanchev/Satellite>
48. <http://del.icio.us/DDanchev/Space>
49. <http://del.icio.us/DDanchev/SPAWAR>
50. <http://www.defenselink.mil/transformation/articles/2006-06/ta062906b.html>
51. <http://del.icio.us/DDanchev/Intelligence>
52. <http://del.icio.us/DDanchev/Terrorism>
53. <http://del.icio.us/DDanchev/Surveillance>
54. <http://del.icio.us/DDanchev/Technology>
55. [http://www.fas.org/blog/secrecy/2006/06/how\\_did\\_us\\_assess\\_iraqi\\_biowea.html](http://www.fas.org/blog/secrecy/2006/06/how_did_us_assess_iraqi_biowea.html)

56. <http://del.icio.us/DDanchev/Intelligence>
57. <http://metasploit.blogspot.com/2006/07/month-of-browser-bugs.html>
58. <http://del.icio.us/DDanchev/Vulnerabilities>
59. <http://del.icio.us/DDanchev/0day>
60. <http://del.icio.us/DDanchev/Metasploit>
61. [http://www.businessweek.com/technology/content/jun2006/tc20060630\\_156285.htm](http://www.businessweek.com/technology/content/jun2006/tc20060630_156285.htm)
62. <http://del.icio.us/DDanchev/IM>
63. <http://del.icio.us/DDanchev/Compliance>
64. <http://www.redherring.com/Article.aspx?a=17471&hed=Trend+Micro+Execs+Face+Probe>
65. <http://del.icio.us/DDanchev/Investing>
66. <http://del.icio.us/DDanchev/AntiVirus>
67. [http://www.boingboing.net/2006/07/05/blast\\_from\\_the\\_past\\_.html](http://www.boingboing.net/2006/07/05/blast_from_the_past_.html)
68. <http://del.icio.us/DDanchev/Defense>
69. <http://del.icio.us/DDanchev/Nuclear>
70. <http://del.icio.us/DDanchev/Technology>
71. [http://www.fas.org/blog/secretcy/2006/07/foia\\_at\\_forty.html](http://www.fas.org/blog/secretcy/2006/07/foia_at_forty.html)



72. <http://del.icio.us/DDanchev/FOIA>
73. <http://www.informationweek.com/story/showArticle.jhtml?articleID=190300177>
74. <http://del.icio.us/DDanchev/Malware>
75. <http://del.icio.us/DDanchev/AntiVirus>
76. <http://theinvisiblethings.blogspot.com/2006/07/blue-pill-hype.html>
77. <http://del.icio.us/DDanchev/Malware>
- 403
78. <http://del.icio.us/DDanchev/Rootkit>
79. <http://del.icio.us/DDanchev/Innovation>
80. <http://www.scmagazine.com/us/news/index.cfm?fuseaction=XCU.News.Article&nNewsid=552938>
81. <http://del.icio.us/DDanchev/Malware>
82. <http://en.apa.az/news.php?id=11697>
83. <http://del.icio.us/DDanchev/Censorship>
84. <http://del.icio.us/DDanchev/Intelligence>
85. <http://del.icio.us/DDanchev/Iran>
86. <http://www.foxnews.com/story/0,2933,201332,00.html>
87. <http://del.icio.us/DDanchev/Intelligence>

88. <http://del.icio.us/DDanchev/Espionage>
89. <http://del.icio.us/DDanchev/Terrorism>
90. <http://del.icio.us/DDanchev/FreeSpeech>
91. <http://arstechnica.com/news.ars/post/20060705-7194.html>
92. <http://del.icio.us/DDanchev/Censorship>
93. <http://del.icio.us/DDanchev/Mobile>
94. <http://www.turkishweekly.net/news.php?id=34295>
95. <http://del.icio.us/DDanchev/Intelligence>
96. <http://del.icio.us/DDanchev/Espionage>
97. <http://del.icio.us/DDanchev/Iran>
98. [http://news.xinhuanet.com/english/2006-07/05/content\\_4798820.htm](http://news.xinhuanet.com/english/2006-07/05/content_4798820.htm)
99. <http://del.icio.us/DDanchev/Intelligence>
100. <http://del.icio.us/DDanchev/Espionage>
101. <http://del.icio.us/DDanchev/CIA>
102. [http://www.pbs.org/newshour/bb/media/july-dec06/nytimes\\_07-05.html](http://www.pbs.org/newshour/bb/media/july-dec06/nytimes_07-05.html)
103. <http://del.icio.us/DDanchev/FreeSpeech>
104. <http://blog.wired.com/27BStroke6/#1516283>

105. <http://del.icio.us/DDanchev/SCADA>
106. <http://del.icio.us/DDanchev/Nuclear>
107. <http://del.icio.us/DDanchev/Cyberterrorism>
108. <http://del.icio.us/DDanchev/Malware>
109. [http://money.cnn.com/2006/07/05/news/companies/coke\\_psi/](http://money.cnn.com/2006/07/05/news/companies/coke_psi/)
110. <http://del.icio.us/DDanchev/Insider>
111. <http://del.icio.us/DDanchev/Espionage>
112. <http://www.viruslist.com/en/analysis?pubid=189801874>
113. <http://del.icio.us/DDanchev/Malware>
114. <http://del.icio.us/DDanchev/Innovation>
115. <http://mdn.mainichi-msn.co.jp/national/news/20060707p2a00m0na005000c.html>
116. <http://del.icio.us/DDanchev/Defense>
117. <http://del.icio.us/DDanchev/Military>
118. <http://cryptome.org/fcc070506.htm>
119. <http://del.icio.us/DDanchev/Security>
120. <http://del.icio.us/DDanchev/Terrorism>
121. <http://del.icio.us/DDanchev/Intelligence>

- 122. <http://del.icio.us/DDanchev/Wiretapping>
- 123. <http://del.icio.us/DDanchev/CALEA>
- 124. <http://del.icio.us/DDanchev/VoIP>
- 125. <http://del.icio.us/DDanchev/Compliance>
- 126. <http://www.qando.net/details.aspx?Entry=4193>
- 127. <http://del.icio.us/DDanchev/Defense>
- 404
- 128. <http://del.icio.us/DDanchev/Military>
- 129. <http://del.icio.us/DDanchev/Reconnaissance>
- 130. <http://www.kcna.co.jp/item/2004/200407/news07/26.htm>
- 131. <http://del.icio.us/DDanchev/Espionage>
- 132. <http://del.icio.us/DDanchev/Military>
- 133. <http://del.icio.us/DDanchev/Reconnaissance>
- 134. <http://www2.csoonline.com/exclusives/column.html?CID=22499>
- 135. <http://del.icio.us/DDanchev/Security>
- 136. <http://del.icio.us/DDanchev/Interview>
- 137. <http://del.icio.us/DDanchev/Leadership>
- 138. <http://www.redherring.com/Article.aspx?a=17494&hed=Google%E2%80%99s+Microsoft+Syndrome>

139. <http://del.icio.us/DDanchev/Vulnerability>
140. <http://del.icio.us/DDanchev/Google>
141. <http://del.icio.us/DDanchev/NewMedia>
142. <http://del.icio.us/DDanchev/Web>
143. <http://www.ft.com/cms/s/42fc828a-0c7a-11db-8235-0000779e2340,s01=1.html>
144. <http://del.icio.us/DDanchev/NewMedia>
145. <http://del.icio.us/DDanchev/Advertising>
146. <http://del.icio.us/DDanchev/Investing>
147. <http://www.eweek.com/article2/0,1759,1986065,00.asp?kc=EWRSS03129TX1K0000614>
148. <http://del.icio.us/DDanchev/Malware>
149. <http://del.icio.us/DDanchev/AntiVirus>
150. <http://del.icio.us/DDanchev/Rootkit>
151. <http://del.icio.us/DDanchev/Technology>
152. <http://www.vnunet.com/vnunet/news/2159880/vpn-market-hit-29bn-2009>
153. <http://del.icio.us/DDanchev/Security>
154. <http://del.icio.us/DDanchev/VPN>
155. <http://del.icio.us/DDanchev/Investing>

156. <http://motoring.reuters.co.uk/reuters/vocmain.jsp?lnk=101&id=1778&desc=%20US%20managers%20accused%20o>

[f%20industrial%20espionage](http://del.icio.us/DDanchev/Espionage)

157. <http://del.icio.us/DDanchev/Espionage>

158. <http://del.icio.us/DDanchev/Insider>

159. <http://www.guardian.co.uk/uklatest/story/0,,5933384,00.html>

160. <http://del.icio.us/DDanchev/Security>

161. [http://www.boston.com/news/nation/articles/2006/07/06/authorities\\_say\\_gangs\\_using\\_internet/](http://www.boston.com/news/nation/articles/2006/07/06/authorities_say_gangs_using_internet/)

162. <http://del.icio.us/DDanchev/PSYOPS>

405

### **Security Research Reference Coverage (2006-07-09 18:27)**

I've recently started getting more requests on participating or guiding to a certain extend, student theses and various

other research papers. There's nothing more pleasant than exchanging points of view, don't preach, but teach

and question everything is what I have in mind. So, I've decided to share some publications featuring some of my

previous papers, and by the way, I'm very near to releasing two research papers on hot topics that emerged during

2006, so stay tuned!

## Online Media

- [1]Quoted in an article by **Arthur G. Insana** for lmediaConnection.com back in 2004, discussing the various threats posed by trojan horses. Trouble is, **I'm no longer affiliated with the company**. Respect the individual!
- Quoted in an article by Bill Brenner on the [2]"Storm Worm" and social engineering when it comes to malware in general
- My paper on the future trends of malware got [3]Slashdotted
- Security.nl covered [4]the International Exploits Shop in an article
- Yet another article at Security.nl this time regarding my [5]future trends of malware paper.
- Marc Olanié at Reseaux-Telecoms.net has been writing lots of articles regarding my research worth going through
- [6]Microsoft, concepteur de virus
- [7]Des truands, des failles, du business...
- [8]Danchev sur l'Achat de failles
- [9]Bientôt, le virus et l'attaque DoS on demand
- [10]Encore et toujours F-Secure/Kaspersky...
- [11]Clusif : le rapport criminalité 2005, chantages et escroqueries

- [12]Le Cyber-Jihad fait trembler l'Amérique
- [13]La vie secrète du phishing : 20/20 en éco et géographie
- [14]Symantec : Boulevard du crime... et au delà

#### Research Papers/Academic

[15]- [16]Future of Malicious Code references my future trends of malware paper. Here's the [17]French version

- [18]Entwurf eines Kunstlichen Immunsystems zur Netzwerkuberwachung auf Basis eines Multi-Agenten-Systems

references future trends of malware

- [19]Limiting Vulnerability Exposure through effective Patch Management: Threat Mitigation Through Vulnerability

Remediation references my best practices on security policies

- [20]Developing a Security Policy refences my paper on security policies

- [21]Policy Review references my paper on security policies

- **Hu Xiaodong**, "[22]Security Centre for an Enterprise thesis", CS Department, Stockholm's University, refer-

ences [23]*Building and Implementing a Successful Information Security Policy*

- **Jinqiao Yu**, "[24]TRINETR: An Intrusion Detection Alert Management and Analysis System dissertation", College of



Engineering and Mineral Resources at West Virginia University, references [25]*Building and Implementing a*

*Successful Information Security Policy*

- **Philippe Farges** and **Annick Tremblet**, "[26]Project on Trojans", Department of Computer Science Linköping Institute of Technology, Sweden, references [27]*The Complete Windows Trojan Paper*

- **Fausi Qattan & Fredrik Thernelius**, "[28]Deficiencies in Current Software Protection Mechanisms and Alternatives 406

for Securing Computer Integrity", Department of Computer and Systems Sciences

Stockholm University - Royal Institute of Technology, references *The Complete Windows Trojan Paper*

- **Computer Knowledge**, "[29]Virus Tutorial" references *The Complete Windows Trojan Paper*

- **Reyes, Juan Carlos**, "[30]Una Aproximación Teórica a la Prevención del Factor Humano en la Seguridad Informatica" , references [31]*Reducing "Human Factor" Mistakes*

- **Rezan Fisli**, "[32]Secure Corporate Communications Over VPN-Based WANs", references [33]*Building and Implementing a Successful Information Security Policy*

- **Vo Khac Thanh**, "[34]An IT security policy framework", Asian Institute of Technology SAT : School of Advanced Technologies, references [35]*Building and Implementing a Successful Information Security Policy*

- **Rohmadi Hidayat**, "[36]Deteksi Trojan Dan Penanganannya", references *The Complete Windows Trojan Paper*

- **Robert J. Kaufman III**, "[37]Susceptibilities Policy Review (Top-Down Methodology) Lesson 7 PPT", The University of Texas at San Antonio, College of Business, references [38]*Building and Implementing a Successful Information*

*Security Policy*

- "[39]Trends of Spyware, Viruses and Exploits", references [40]*Malware - it's getting worse*

- **Steven M. Michnick**, "[41]Information Security Framework for Small and Medium Sized Businesses", references

[42]*Passwords - Common Attacks and Possible Solutions*

- **Samer Catalan**, "[43]Trojan Horses", RWTH Aachen University, references *The Complete Windows Trojan Paper*

- **Stephen M. Specht** and **Ruby B. Lee**, "[44]Distributed Denial of Service: Taxonomies of Attacks, Tools, and Countermeasures", Proceedings of the 17th International Conference on Parallel and Distributed Computing Systems,

International Workshop on Security in Parallel and Distributed Systems, references *The Complete Windows Trojan*

*Paper*

- **Delwyn Lee, Adam Marks, David Bell**, "[45]Student Residence Secure Solutions Analysis of ResNet Security",

references [46]*Building and Implementing a Successful Information Security Policy*

- **Clarissa L. Evans Brown**, “[47]A Policy to prevent outsider attacks on the local network”, GSEC Practical Assignment, references [48]*Building and Implementing a Successful Information Security Policy*

- **Hatim Ali Badr**, “[49]Online home users Defense in Depth”, GIAC Practical Assignment, references *The Complete Windows Trojan Paper*

- **Tim Strong**, “[50]PestPatrol in a Corporate Environment: A Case Study in Information Security” – GIAC Practical Assignment, references *The Complete Windows Trojan Paper's Future of Trojans section*

- **Sorcha Canavan**, “[51]An Information Policy Development Guide for Large Companies” – GSEC, Practical Assignment, references [52]*Building and Implementing a Successful Information Security Policy*

- **Gregory R. Panakkal**, “[53]Advanced Survival Techniques in Malware”, Cochin University of Science and Technology, references *The Complete Windows Trojan Paper*

- **Michael D. Thacker**, “[54]Effective Security Policy Management” – Virus Bulletin 2005 Conference, references

[55]*Building and Implementing a Successful Information Security Policy*

- My paper regarding security policies has been discussed in a [56]network security course at the **George Ma-**

**son University**

- University of Melbourne's [57]Network Security Course teaches on my security policies publication
- [58]University of Houston are giving assignments on my security policies publication

407

- **Tim Lackorzynski**, "[59]Future Trends of Malware PPT", Fakultät Informatik, Technische Universität Dresden,

[60]Proseminar Dependable Systems is discussing my "[61]Malware - Future Trends" research

- **Widener University** have included my "[62]Steganography and Cyber Terrorism Communications" in their

[63]forensics course reading materials

1. <http://www.imediaconnection.com/content/4100.asp>

2. [http://searchsecurity.techtarget.com/columnItem/0,294698,sid14\\_gci1240768,00.html](http://searchsecurity.techtarget.com/columnItem/0,294698,sid14_gci1240768,00.html)

3. <http://it.slashdot.org/article.pl?sid=06/01/11/1323212&tid=172>

4. [http://www.security.nl/article/13099/1/Internationale\\_Exploit\\_Shop\\_levert\\_0days\\_op\\_bestelling.html](http://www.security.nl/article/13099/1/Internationale_Exploit_Shop_levert_0days_op_bestelling.html)

5. [http://www.security.nl/article/12808/1/De\\_toekomst\\_van\\_malware.html](http://www.security.nl/article/12808/1/De_toekomst_van_malware.html)

6. <http://securite.reseaux-telecoms.net/actualites/lire-microsoft-concepteur-de-virus-12754.html>
7. <http://securite.reseaux-telecoms.net/actualites/lire-des-truands-des-failles-du-business-13219.html>
8. <http://securite.reseaux-telecoms.net/actualites/lire-danchev-sur-l-achat-de-failles-12703.html>
9. <http://securite.reseaux-telecoms.net/actualites/lire-bientot-le-virus-et-l-attaque-dos--on-demand-12182.html>
10. <http://securite.reseaux-telecoms.net/actualites/lire-encore-et-toujours-f-secure-kaspersky-15444.html>
11. <http://securite.reseaux-telecoms.net/actualites/lire-clusif-le-rapport--criminalite-2005--chantages-et-escroqueries-12230.html>
12. <http://securite.reseaux-telecoms.net/actualites/lire-le-cyber-jihad-fait-trembler-l-amerique-15053.html>
13. <http://securite.reseaux-telecoms.net/actualites/lire-la-vie-secrete-du-phishing-20-20-en-eco-et-geographe-15609.html>
14. <http://securite.reseaux-telecoms.net/actualites/lire-symantec-boulevard-du-crime-et-au-dela-15831.html>
15. [http://www.rcmp-grc.gc.ca/tsb/pubs/it\\_sec/r2-002\\_f.pdf](http://www.rcmp-grc.gc.ca/tsb/pubs/it_sec/r2-002_f.pdf)

16. [http://www.rcmp-grc.gc.ca/tsb/pubs/it\\_sec/r2-002\\_e.pdf](http://www.rcmp-grc.gc.ca/tsb/pubs/it_sec/r2-002_e.pdf)
17. [http://www.rcmp-grc.gc.ca/tsb/pubs/it\\_sec/r2-002\\_f.pdf](http://www.rcmp-grc.gc.ca/tsb/pubs/it_sec/r2-002_f.pdf)
18. [http://www.dai-labor.de/fileadmin/files/publications/Diplomarbeit\\_KL.pdf](http://www.dai-labor.de/fileadmin/files/publications/Diplomarbeit_KL.pdf)
19. <http://singe.za.net/masters/thesis/Dominic%20White%20-%20MSc%20-%20Patch%20Management.pdf>
20. <http://www.andrew.cmu.edu/course/95-841/notes/DevSecPolicy.ppt>
21. <http://faculty.business.utsa.edu/rkaufman/SRALsn7.ppt>
22. <http://www.dsv.su.se/research/seclab/pages/pdf-files/2005-x-248.pdf>
23. [http://niatec.isu.edu/pdf/security\\_policy.pdf](http://niatec.isu.edu/pdf/security_policy.pdf)
24. <http://siplab.csee.wvu.edu/research/TRINETR/Dissertation.pdf>
25. [http://www.net-security.org/dl/articles/security\\_policy.pdf](http://www.net-security.org/dl/articles/security_policy.pdf)
26. <http://www.ida.liu.se/%7ETDDC03/oldprojects/2004/final-projects/prj028.pdf>
27. [http://www.windowsecurity.com/whitepapers/The\\_Complete\\_Windows\\_Trojans\\_Paper.html](http://www.windowsecurity.com/whitepapers/The_Complete_Windows_Trojans_Paper.html)
28. <http://www.dsv.su.se/research/seclab/pages/pdf-files/04-34.pdf>

29. [http://www.coa.edu/assets/it\\_downloads/vtutor.pdf](http://www.coa.edu/assets/it_downloads/vtutor.pdf)
30. <http://www.seltika.com/archivos/Aproximaci%C3%B3n%20Te%C3%B3rica%20a%20la%20prevenci%C3%B3n%20del%20Factor%20Humano%20V0.1.pdf>
31. [http://www.windowsecurity.com/articles/Reducing\\_Human\\_Factor\\_Mistakes.html](http://www.windowsecurity.com/articles/Reducing_Human_Factor_Mistakes.html)
32. [http://www.nada.kth.se/utbildning/grukth/exjobb/rapportlistor/2005/rapporter05/fisli\\_rezan\\_05182.pdf](http://www.nada.kth.se/utbildning/grukth/exjobb/rapportlistor/2005/rapporter05/fisli_rezan_05182.pdf)
33. <http://www.packetstormsecurity.org/papers/general/security-policy.pdf>
34. <http://www.library.ait.ac.th/ThesisSearch/summary/Vo%20Khac%20Thanh.pdf>
35. [http://www.infosecwriters.com/text\\_resources/pdf/security-policy.pdf](http://www.infosecwriters.com/text_resources/pdf/security-policy.pdf)
36. <http://budi.insan.co.id/courses/el7010/dikmenjur-2004/rohmedi-report.pdf>
37. <http://faculty.business.utsa.edu/rkaufman/SRALsn7.ppt>
38. <http://niatec.isu.edu/pdf/security-policy.pdf>
39. [http://www.simson.net/ref/2005/csci\\_e-170/p1/king.pdf](http://www.simson.net/ref/2005/csci_e-170/p1/king.pdf)

40.

[http://www.windowsecurity.com/articles/Malware\\_Getting\\_Worse.html](http://www.windowsecurity.com/articles/Malware_Getting_Worse.html)

41.

<http://kuscholarworks.ku.edu/dspace/bitstream/1808/970/1/Michnick,+Steven+M.+EMGT+Field+Project.pdf>

408

42. <http://www.windowsecurity.com/articles/Passwords-Attacks-Solutions.html>

43. <http://www-i4.informatik.rwth-aachen.de/lufg/teaching/ss2004/dependability-seminar/paper/final8.pdf>

44.

<http://palms.ee.princeton.edu/PALMSopen/DDoS%20Final%20PDCS%20Paper.pdf>

45. <http://web.syr.edu/%7Eatmarks/docs/623/Student.doc>

46.

<http://www.packetstormsecurity.org/papers/general/security-policy.pdf>

47.

<http://cnscenter.future.co.kr/resource/security/consulting/1362.pdf>

48.

<http://www.packetstormsecurity.org/papers/general/security-policy.pdf>

49.

[http://www.giac.org/certified\\_professionals/practicals/gsec/2](http://www.giac.org/certified_professionals/practicals/gsec/2)



[780.php](#)

50.

[http://www.giac.org/certified\\_professionals/practicals/gsec/2314.php](http://www.giac.org/certified_professionals/practicals/gsec/2314.php)

51.

<http://www.cbts.cinbell.com/test/doc/largecompanysecuritypolicy.pdf>

52.

<http://www.packetstormsecurity.org/papers/general/security-policy.pdf>

53. [http://www.infogreg.com/articles-dir/export/seminar\\_report\\_astim.pdf](http://www.infogreg.com/articles-dir/export/seminar_report_astim.pdf)

54.

[http://www.virusbtn.com/conference/vb2005/abstracts/Michael\\_D\\_ThackerCorpWeds1620.xml](http://www.virusbtn.com/conference/vb2005/abstracts/Michael_D_ThackerCorpWeds1620.xml)

55.

<http://www.packetstormsecurity.org/papers/general/security-policy.pdf>

56. <http://teal.gmu.edu/%7Egmartin/fall05/tcom562-f05.htm>

57.

[http://www.muprivate.edu.au/fileadmin/SOE/ecrime/Weekly/sally/SE5013\\_readings.doc](http://www.muprivate.edu.au/fileadmin/SOE/ecrime/Weekly/sally/SE5013_readings.doc)

58.

[http://dcm.cl.uh.edu/nsfsecurity/public/Modules/AYang\\_Module/admi1/Assignment1/Admi1Assign1.html](http://dcm.cl.uh.edu/nsfsecurity/public/Modules/AYang_Module/admi1/Assignment1/Admi1Assign1.html)

59. <http://wwwse.inf.tu-dresden.de/wiki/images/f/f6/PRO-TimLackorzynski.pdf>

60. [http://wwwse.inf.tu-dresden.de/wiki/index.php/Proseminar\\_Topics](http://wwwse.inf.tu-dresden.de/wiki/index.php/Proseminar_Topics)

61. <http://www.packetstormsecurity.org/papers/general/malware-trends.pdf>

62. <http://ddanchev.blogspot.com/2006/08/steganography-and-cyber-terrorism.html>

63. <http://cs.widener.edu/%7Eyanako/html/courses/Fall06/forensics/coursemat.html>

409



### **South Korea's View on China's Media Control and Censorship (2006-07-10 22:21)**

[1]

Got bored of [2]China's Internet censorship efforts, and its [3]interest to control mobile communications as well?

I haven't, and I doubt I ever will given China is among the many other [4]countries on the world's map actively

restricting access to information, and, of course, controlling the way it reaches the final audience – if it does.

A recent article at [5]The Korean Times, makes some very good points on the cons of censoring the reporting

of "sudden events", and the typical for a (modern) communist type of government, total centralization. It emphasises on how :

*" Beijing's approach is fundamentally flawed. The news media is a positive force in society. A free press is necessary to keep the government on its toes, especially when the government itself is not accountable to the public.*

*Restricting the press will result in a public that is kept in the dark and in local governments whose excesses will no longer be subject to scrutiny.*

*Beijing should understand that many of today's problems today stem from abusive local officials. Premier Wen*

*Jiabao acknowledged at a press conference in March that some local governments have infringed upon the legitimate*

*rights and interests of the people, and social conflicts have subsequently occurred.*

*In this struggle between victimized farmers and avaricious officials, the press—and the central government—*

*are on the same side. Muzzling the press will only deprive the victims of a powerful champion while enabling grasping*

*officials to line their pockets without fear of being exposed. Surely, this cannot be what the Chinese government wants. "*

In case of a "sudden event" I feel they'd rather be winning time compared to keeping it quiet, then again I

guess ruling one of the largest nation in the world while trying to maintain stability - [6]FDI matters folks - is a

daunting task, but one not necessarily having to do with ignoring the situation. Government accountability and

possible changes in voting attitudes in China don't exist, mainly because there isn't any other party, but THE party,

therefore historical (under)performance doesn't count at all.

In comparison, whereas Chinese citizens suffer from the lack of information or the blocked access to it, in the

U.S there's [7]a controversial debate going on regarding over-performing investigative journalists revealing details

thought to be sensitive to national security, and the overall availability of potentially sensitive information to the

general public. The problem isn't the "leak" as it's a common sense practice, but the publicity it got in the post 9/11, privacy-preserving society - or at least one [8]trying to. Doesn't really matter if [9]the FOIA turned forty,

[10]"redacting" is often misspelled for censorship, [11]in between the lines of personal and sensitive information.

At the bottom line, government practices' transparency with the help of the media watchdogs, a government incapable of knowing the exact state of a situation by itself, or the notion of too much publicly available information

in today's OSINT world, up to you to decide, just don't rule, run business, or blog, by excluding the middle, or you'll

sooner or later face with it in one way or another.

1. <http://photos1.blogger.com/blogger/1933/1779/1600/Censorship.jpg>
2. <http://ddanchev.blogspot.com/2006/02/chinese-internet-censorship-efforts.html>
3. <http://ddanchev.blogspot.com/2006/07/chinas-interest-of-censoring-mobile.html>
4. <http://ddanchev.blogspot.com/2006/06/worlds-internet-censorship-map.html>
5. <http://times.hankooki.com/lpage/opinion/200607/kt2006070920210454310.htm>
6. <http://www.fdi.gov.cn/main/indexen.htm>
7. [http://www.pbs.org/newshour/bb/media/july-dec06/nytimes\\_07-05.html](http://www.pbs.org/newshour/bb/media/july-dec06/nytimes_07-05.html)
8. <http://ddanchev.blogspot.com/2006/06/all-your-confidentiality-are-belong-to.html>
9. [http://www.fas.org/blog/secretcy/2006/07/foia\\_at\\_forty.html](http://www.fas.org/blog/secretcy/2006/07/foia_at_forty.html)

10.

<http://www.contracostatimes.com/mld/cctimes/14952653.htm>

11. <http://ddanchev.blogspot.com/2006/04/in-between-lines-of-personal-and.html>

411

x

## **India's Espionage Leaks (2006-07-10 23:36)**

[1]

You may find this brief overview of [2]Indian security's leaky past cases informative :

- " **Defence Research and Development Organisation (DRDO) hard drive theft.**

*The hard drives were stolen*

*from the offices of the Scientific Analyses Group (SAG) and the Institute for System Studies and Analyses (ISSA)*

*inside the DRDO complex. The SAG is responsible for cryptography. In other words, all codes and cyphers to ensure*

*communication security for the defence forces have an SAG stamp. The ISSA, on the other hand, analyses competing*

*weapons systems for induction into the armed forces. "*

- " **Rabinder Singh.** *It is said there was a question mark over his reliability since the early 1990s when he began an operation for the collection of intelligence about US*

*government activities in South Asia through a sister of his, who was employed in a sensitive US agency with links to the CIA. "*

*- " **Rattan Sehgal.***

*The IB's counter-intelligence division reportedly found that a woman CIA officer posted in*

*the US embassy was in contact with government servants and others on a mobile telephone, allegedly registered in*

*the name of their boss, the suspect IB officer. "*

*- " **KV Unnikrishnan.** During those jaunts in Singapore, compromising photographs of the stewardess and her lover were taken. These photographs and other documents were recovered by mid '86 and it was learnt that*

*Unnikrishnan was working for the CIA. "*

*- " **Larkins Brothers.** The Larkins' interrogations led to the arrest of Singh and it was found that Jockey and Bud were CIA operatives. "*

*- " **Samba Spy Case.** By 1974, he began working for its army's Field Intelligence Unit at Sialkot on a regular basis. In the June of 1975, Dass was arrested on suspicion of espionage but by then he had persuaded some of his*

*colleagues (including a certain Aya Singh) to become accomplices. "*

Understanding the past means predicting or at least constructively speculating on the future.

Insider leaks

due to HUMINT recruitment activities may seem to have vanished given the increasing number of IT-dependent infrastructures and the insecurities their connectivity brings - [3]SIGINT taking over [4]HUMINT [5]espionage. While [6]modern spy gadgets remain trendy, this very same connectivity has resulted in various [7]hacktivism tensions in the past, namely the [8]India vs Pakistan [9]cyberwar, and, of course, [10]MilW0rm's infamous speculation on [11]breaching India's Bhabha Atomic Research Center through the use of U.S military servers as [12]island-hopping points.

Office surveillance graph courtesy of [13]BugSweeps.

1. [http://photos1.blogger.com/blogger/1933/1779/1600/office\\_espionage.jpg](http://photos1.blogger.com/blogger/1933/1779/1600/office_espionage.jpg)
2. [http://www.hindustantimes.com/news/181\\_1739400,0008.htm](http://www.hindustantimes.com/news/181_1739400,0008.htm)
3. <http://en.wikipedia.org/wiki/SIGINT>
4. <http://en.wikipedia.org/wiki/HUMINT>
5. <http://del.icio.us/DDanchev/Espionage>
6. [http://www.forbes.com/technology/2006/04/15/intelligence-spying-gadgets\\_cx\\_lh\\_06slate\\_0418tools.html](http://www.forbes.com/technology/2006/04/15/intelligence-spying-gadgets_cx_lh_06slate_0418tools.html)



7. <http://ddanchev.blogspot.com/2006/07/hackivism-tensions-israel-vs.html>

8. <http://www.wired.com/news/politics/0,1283,40789,00.html>

9. <http://www.cnn.com/TECH/computing/9910/08/pakistani.hack/>

10. <http://www.rediff.com/computer/1998/jun/09barc.htm>

11. <http://www.exn.ca/Stories/1998/06/08/60.asp>

412

12. [http://en.wikipedia.org/wiki/Island\\_hopping](http://en.wikipedia.org/wiki/Island_hopping)

13. <http://www.bugsweeps.com/info/spytech.html>

413



## **Spreading Psychological Imagination Streams (2006-07-14 16:54)**

[1]

Wish I could reference all the copywriting materials I've ever written and got commissioned for, but I'd rather we play a "words creativity" game. There's no better personal benchmark for keeping yourself in a good shape, and most importantly, indirectly summarizing what's going on in my head at a particular moment, than of coming up with random/instant sentences out of key words I come across

to while reading an article. Enjoy, and remember a key word is worth a thousand sentences!

**Wordlist :**

- Breed
- Cupidity
- Intermediaries
- Powerhouse
- Quadrupled
- Commodities
- Proliferation
- Liquidity
- Licensing
- The arms race
- Competitiveness

**Outcome :**

- The boom of the Web, and the now experienced dotcom industry, has generated a whole new **breed** of wannabe entrepreneurs
- From some people's point of view, **cupidity** is just profit-maximization

- Among Dell's most important strategic objectives were to cut the **intermediaries**, thereby lowering the final

price of a PC and stealing market share. Trouble is, hardware turned into a commodity these days

- AOL - the Internet's **powerhouse** from the early days of the Web itself, got the necessary attention from

both, Microsoft, and Google due to the highly competitive atmosphere the rivals created. Eyeballs converted into

revenue sources

- Since the standardization of advertising creative, online ad revenues **quadrupled**

414

- **Commodity** markets are the true nirvana when it comes to betting and the potential to gain enormous returns in a short period of time

- The **proliferation** of false statements by the Senator, has resulted in decline in our sales due to privacy con-

cerns

- Achieving **liquidity** should be issue number one for a less capital goods intensive organization

- **Licensing** not only cuts R &D costs, it also provides a company with the ability to gain competitive advantage, and improve its value-added proposition next to its rivals' ones

- The **arms race** in patents and brands registering across the world, has resulted in a great deal of still unused, and in

beta mode of testing technologies and names

- The **competitiveness** in the Business Services market segment that IBM was seeking, is among the main reasons for their sale of the company's entire PC units division – today's Lenovo

An analysis of **hard cover security ads from the most popular business magazines** will follow at the beginning of the week. Actual shots, the messages themselves and detailed recommendations are to be included as well.

Information security and business always tend to intersect, excluding one is like ignoring the other.

1.  
<http://photos1.blogger.com/blogger/1933/1779/1600/creativity.jpg>

415



**North Korea's Cyber Warfare Unit 121 (2006-07-16 01:08)**

[1]

In a previous post, "[2]Who's Who in Cyber Warfare" I commented on a very informative [3]research on the topic, and pointed out that :

*" Technology as the next Revolution in Military Affairs (RMA) was inevitable development, what's important to*

*keep in mind is knowing who's up to what, what are the foundations of their military thinking, as well as who's*

*copying attitude from who. Having the capacity to wage offensive and defense cyber warfare is getting more*

*important, still, military thinkers of certain countries find [4] network centric warfare or total renovation of [5] C4I communications as the panacea when dealing with their about to get scraped conventional weaponry systems.*

*Convergence represents countless opportunities for waging Cyber Warfare, offensive one as well, as I doubt there*

*isn't a country working on defensive projects. "*

Recently, there's been some movement from [6]North Korea's Cyber Warfare unit 121, one that :

*" North Korea set up about eight years ago with some 1,000 personnel, said the intelligence official, who de-*

*clined to be named because it was the agency's policy to remain anonymous. The North's operation, called unit 121,*

*"has hacked into the South Korean and U.S. Defense Department" and has caused much damage in the South, the official said without elaborating."*

[7]According to [8]numerous [9]articles on recent "anomalies" at unclassified U.S state department systems,

these might actually have to do with the group's actions itself – quite a momentum to take advantage of, isn't it?

Any country's interest in [10]establishing [11]cyber war forces shouldn't come as a surprise to anyone. But while

North Korea is trying to balance its military powers through asymmetric and cyber warfare approaches given its

outdated conventional weaponry thinking, I feel the real beast to worry about is China, who's sneakily hiding behind

its currently strategic economic position. As the latest report on "[12]Military Power of the People's Republic of

China 2006" points out :

*" The People's Liberation Army (PLA) has established information warfare units to develop viruses to attack enemy computer systems and networks, and tactics and measures to protect friendly computer systems and networks. "*

Taiwan is reasonably taking note on China's [13]historical [14]cyber warfare actions and has [15]recently initi-

ated its first cyber war game simulating attack from China :

*" The drill, part of the island's annual major war game Hankuang No. 22, was held Wednesday and Thursday to intercept, block and counter a possible Chinese cyber attack of Taiwan's major computer network to paralyze the island's intranet operation, the Central News Agency quoted an unnamed defence source as saying. "*

Let's don't forget the use and abuse of island hopping points fueling further tensions in key regions and abus-

ing the momentum itself, [16]physically locating a network device in the future IPv6 network space is of key interest

to all parties.

War room courtesy of Northrop Grumman.

### **Related resources:**

[17]Information Warfare

[18]Cyber Warfare

1.

[http://photos1.blogger.com/blogger/1933/1779/1600/cwin\\_cutout.jpg](http://photos1.blogger.com/blogger/1933/1779/1600/cwin_cutout.jpg)

2. <http://ddanchev.blogspot.com/2006/05/whos-who-in-cyber-warfare.html>

416

3. <http://www.ists.dartmouth.edu/directors-office/cyberwarfare.pdf>

4. [http://www.vodium.com/MediapodLibrary/index.asp?library=dod\\_ofc\\_incw&SessionArgs=0A1U0000000100000111](http://www.vodium.com/MediapodLibrary/index.asp?library=dod_ofc_incw&SessionArgs=0A1U0000000100000111)

5.

[http://en.wikipedia.org/wiki/Command,\\_control,\\_and\\_communications](http://en.wikipedia.org/wiki/Command,_control,_and_communications)

6. <http://www.smh.com.au/news/Technology/NKorea-operates-cyber-warfare-unit-to-disrupt-SKoreas-militarycommand>

[nd-official/2006/07/12/1152637718059.html](http://www.abc.net.au/news/2006/07/12/1152637718059.html)

7. <http://www.eweek.com/article2/0,1895,1987870,00.asp>

8. <http://www.informationweek.com/news/showArticle.jhtml?articleID=190303153>

9. <http://abcnews.go.com/Politics/wireStory?id=2184451&CMP=OTC-RSSFeeds0312>

10. <http://www.strategypage.com/dls/articles/200561415936.asp>

11. <http://www.wired.com/news/politics/0,1283,59043,00.html>

12. <http://www.globalsecurity.org/military/library/report/2006/2006-prc-military-power.htm>

13. <http://english.chosun.com/w21data/html/news/200407/200407150028.html>

14. <http://www.taipeitimes.com/News/taiwan/archives/2006/06/19/2003314414>

15. [http://tech.monstersandcritics.com/news/article\\_1180816.php/Taiwan\\_stages\\_cyber-war\\_game\\_simulating\\_attack\\_from\\_China](http://tech.monstersandcritics.com/news/article_1180816.php/Taiwan_stages_cyber-war_game_simulating_attack_from_China)

16. <http://www.caida.org/~yoshi/KoBrCl05PDF-hires.pdf>

17. <http://del.icio.us/DDanchev/InformationWarfare>

18. <http://del.icio.us/DDanchev/Cyberwarfare>





## **Scientifically Predicting Software Vulnerabilities (2006-07-16 02:09)**

[1]

I recently came across to a research on "[2]Modeling the Vulnerability Discovery Process" discussing :

*" A few models for the vulnerability discovery process have just been published recently. Such models will al-*

*low effective resource allocation for patch development and are also needed for evaluating the risk of vulnerability exploitation. Here we examine these models for the vulnerability discovery process. The models are examined both*

*analytically and using actual data on vulnerabilities discovered in three widely-used systems. The applicability of the proposed models and significance of the parameters involved are discussed. The limitations of the proposed models*

*are examined and major research challenges are identified.*  
"

A [3]handy summary of the report emphasises on how :

*" The Alhazmi-Malaiya Logistic model has already seen success in its predictions:*

*- In 2005, it predicted the number of vulnerabilities discovered in Windows XP would grow rapidly. It has in-*

*deed grown from 88 in January 2005 to 173 by the latest count, making the vulnerability density of XP comparable to*

*that of earlier version of Windows.*

*- The model predicted that very few new vulnerabilities will be found in Red Hat Linux 6.2, and the number*

*has stayed unchanged at 117.*

*- It predicted that the number of vulnerabilities of Windows 2000 will eventually range from 294 to 410. At*

*that time of the prediction, the number was 172; it now is 250, and vulnerabilities are still being found. "*

Remember the [4]U.S DHS's \$1.24M bug hunt funding, that came up with a [5]single X11 vulnerability? Money well spent for sure.

**HD Moore** who's [6]obviously getting efficient, the potential of contests, futures market models, and my spec-

ulation on "every day there's a new 0day in the wild" ruin the effect of any model. Assuming no external factors influence the process, and the rest remain static - while they rarely do - it's a great initiative, still, more of a

scientifically shooting into the dark one, given the great deal of uncertainties, and decentralized model of discovering, reporting, using and abusing vulnerabilities. If historical performance matters and can act as a key indicator for

predicting the future, I wonder would MACs lack of vulnerabilities continue to generate hype, it's more of a "lack of incentives to find some" type of issue. Today's vibrant vulnerability research intrigue is indeed capable of ruining any model.

I also came across to a [7]great point, indicating that :

*" After the first week of flaws were released, one online miscreant from Russia shot off an e-mail to Moore, complaining that he had outed a vulnerability the Russian had been exploiting, Moore said.*

*"The black hats don't like that the fact that this is public because they have been using these bugs," Moore said. "By dumping out the bugs on the community, I'm clearing the air and letting the good guys know what others are doing. "*

From my point of view, the existence and usefulness of Metasploit is precisely the same type of dilemma whether

citizens should be allowed to carry guns for self-protection or blindly rely on 500 police officers for 500,000 people.

Hopefully, with initiatives like the Month of the Browser bug ones, we would inevitably break through the "yet

another 0day, where's my patch dude? type of security issues to deal with. At the bottom line that's a single, efficient security researcher who's definitely working on building more awareness on what the corporate trolls are ignoring

418

for the sake of their product portfolio diversification.

It's also interesting to mention on the emerging [8]underground 0bay model for selling 0day vulnerabilities

:

*" Cyber crooks are not hesitant to make such open declarations of illicit intent because of the anonymity of-*

*fered by the Internet. Some have had the gall to try and peddle their information on popular online auction sites such as eBay. Last December eBay pulled an ad that was selling vulnerability information about Microsoft's spreadsheet*

*program Excel. That was a bold, if foolhardy, move on the part of the seller, because eBay is hardly blackmarket at*

*all, said Ross Armstrong, senior analyst at technology consultancy firm Info-Tech Research Ltd. in London, Ont. "*

and its corporate form, on which [9]Sergio Hernando was kind enough to point me to.

[10]The VulnDisco

Pack Professional :

- *contains more than 80 exploits*
- *each month about 5-10 new exploits are made available in the form of updates*
- *VulnDisco Pack Professional licenses are not limited to a number of seats*

and you can actually see an [11]OpenLDAP 0day exploit in action for yourself.

Metasploit image courtesy of [12]Metasploit's blog.

## **Related resources and posts:**

[13]Vulnerabilities

[14]0day

[15]Was the WMF vulnerability purchased for \$4000?!

[16]0bay - how realistic is the market for security vulnerabilities?

[17]Where's my 0day, please?

[18]Delaying Yesterday's "0day" Security Vulnerability

[19]Shaping the Market for Security Vulnerabilities Through Exploit Derivatives

[20]Getting paid for getting hacked

1.

[http://photos1.blogger.com/blogger/1933/1779/1600/Metasploit\\_world.png](http://photos1.blogger.com/blogger/1933/1779/1600/Metasploit_world.png)

2. <http://portal.acm.org/affiliated/citation.cfm?id=1104997.1105240&coll=portal&dl=ACM&CFID=151515>

[15&CFTOKEN=6184618](http://portal.acm.org/affiliated/citation.cfm?id=1104997.1105240&coll=portal&dl=ACM&CFID=151515)

3. <http://www.physorg.com/news70807349.html>

4. <http://osvdb.org/blog/?p=83>

5. <http://www.eweek.com/article2/0,1759,1956652,00.asp>

6. <http://metasploit.blogspot.com/2006/07/month-of-browser-bugs.html>

7. <http://www.securityfocus.com/news/11400>

8. <http://www.itworldcanada.com/a/Daily-News/3d3a7274-7f3c-48e7-9151-92a65cdac99d.html>
9. <http://www.sahw.com/wp/archivos/2006/07/14/vulIndisco-pack-professional-de-compras-por-el-lado-oscuro/>
10. [http://www.gleg.net/vulIndisco\\_pack\\_professional.shtml](http://www.gleg.net/vulIndisco_pack_professional.shtml)
11. [http://www.gleg.net/flash/vulIndisco\\_openldap.html](http://www.gleg.net/flash/vulIndisco_openldap.html)
12. <http://metasploit.blogspot.com/>
13. <http://del.icio.us/DDanchev/Vulnerabilities>
14. <http://del.icio.us/DDanchev/0day>
15. <http://ddanchev.blogspot.com/2006/01/was-wmf-vulnerability-purchased-for.html>
16. <http://ddanchev.blogspot.com/2005/12/0bay-how-realistic-is-market-for.html>
17. <http://ddanchev.blogspot.com/2006/03/wheres-my-0day-please.html>

419

18. <http://ddanchev.blogspot.com/2006/05/delaying-yesterdays-0day-security.html>
19. <http://ddanchev.blogspot.com/2006/05/shaping-market-for-security.html>
20. [http://ddanchev.blogspot.com/2006/03/getting-paid-for-getting-hacked\\_17.html](http://ddanchev.blogspot.com/2006/03/getting-paid-for-getting-hacked_17.html)

420



## **Weaponizing Space and the Emerging Space Warfare Arms Race (2006-07-16 14:50)**

[1]

Satellites Jamming, Hijacking, Space SIGINT, Space Kill Vehicles are just the tip of the iceberg in the ongoing

weaponization of Space. In previous posts "[2]Who needs nuclear weapons anymore?", "[3]EMP warfare - Electronic Domination in Reverse", and "[4]Is a Space Warfare arms race really coming?" I expressed my opinion on the current and emerging efforts to install and experiment with space weapons, and mostly emphasized on the major

problem - the arms race fear itself. What's also worth mentioning is how the original [5]anti-missile defense system

Star Wars, transformed from a defensive, to an offensive tool for warfare. SFAM at the [6]CyberpunkReview.com

made a [7]good comment :

*" Weaponizing space when there really isn't any competitor is a really bad idea. Truly though, the issue that*

*obfuscates things is the US military's change from a threat-based acquisition system (where weapon systems were*

*acquired to combat specific and verifiable threats) to a capability-based acquisition system is the problem. The*

*switch to a capability-based system, being divorced from threats (since the Wall fell, most of the threats did as well), can find justification for new weapon systems even if there isn't a verifiable enemy or even a proven, irreplaceable need in warfare for the technology. Case in point - nobody is challenging the US for air supremacy, yet we have*

*massively expensive acquisitions underway for the F-22 (which should have been killed in 1991) and the F-35 (Joint Strike Fighter). "*

Just came across to a great initiative aiming to act as a facilitator for debating the problem. The [8]SpaceDebate.org aims to :

*" expand the debate on the weaponization of space through a collaborative wiki-like tool for structured debate*

*on a topic. You can learn more by taking the [9] quick tour, reading the [10] aboutpage, or browsing our [11] frequently asked questions. You can also jump into the debate by browsing our [12] argument list or one of the [13] positions"*

I feel there's a more serious problem we should be discussing for the time being compared to the world's su-

per powers waging wars in space, and it's called Near Earth Object Protection - there's even a [14]distributed client

for tracking the hazard posed by NEOs. For instance, consider the following [15]alternatives for combating the real

threat in space - the universe itself :



*" There's been no shortage of ideas how to fend off unfriendly fire from the cosmos: laser beams, [16] space tugboats, [17] gravity tractor, and solar sails for example, as well as using powerful anti-NEO bombs, conventional as well as nuclear. Ailor, also Director of The Aerospace Corporation's Center for Orbital and Reentry Debris Studies, told SPACE.com that creative ways to deflect Earth-harming NEOs are far from being exhausted. People have put a lot of concepts on the table over time, Ailor said. Now we're beginning to try and develop an organized way of looking at those things and finding out which ones are really viable in the short-term, medium-term, and what technologies do we need to protect and develop for the long-term as well. "*

[18]

I've always thought the human race is an experiment of a [19]super intelligent race trying to figure out how long it's gonna take us to self-destroy our kind. In case you're interested in the current situation on space warfare, you can also go through the [20]Space Security 2006 book (111 pages), and [21]previous editions as well.

An excerpt from the [22]executive summary :

*" A growing number of states, led by China, Russia, the US, and key European states, increasingly emphasize the use of space systems to support national security. Dependence on these systems has led several states to view*

*space assets as critical national security infrastructure. US military space doctrine has also begun to focus on the need for "counterspace operations" to prevent adversaries from accessing space. Building on existing trends, in 2005*

*actors that included the EU, India, Israel, and Japan placed more emphasis on the national security applications of*

421

*space. Israel and Japan introduced plans to boost surveillance capabilities from space. India's Air Force urged the government to set up a Strategic Aerospace Command to better develop military space capabilities. "*

Don't look for enemies where there aren't still any, but deal with the real space threat. Camouflage, Conceal-

ment, and Deception (CC &D) techniques table courtesy of FAS's "[23]Threats to United States Space Capabilities"

### **Related resources:**

[24]Space

[25]SPAWAR

1.

<http://photos1.blogger.com/blogger/1933/1779/1600/Space%20Weapons.jpg>

2. <http://ddanchev.blogspot.com/2006/02/who-needs-nuclear-weapons-anymore.html>

3. <http://ddanchev.blogspot.com/2006/05/emp-attacks-electronic-domination-in.html>

4. <http://ddanchev.blogspot.com/2006/03/is-space-warfare-arms-race-really.html>
5. [http://en.wikipedia.org/wiki/Strategic\\_Defense\\_Initiative](http://en.wikipedia.org/wiki/Strategic_Defense_Initiative)
6. <http://www.cyberpunkreview.com/>
7. <http://ddanchev.blogspot.com/2006/03/is-space-warfare-arms-race-really.html>
8. <http://www.spacedebate.org/>
9. <http://www.spacedebate.org/tour/>
10. <http://www.spacedebate.org/about>
11. <http://www.spacedebate.org/help/>
12. <http://www.spacedebate.org/arguments/>
13. <http://www.spacedebate.org/positions/>
14. <http://orbit.psi.edu/>
15. [http://www.space.com/news/060628\\_neo\\_workshop.html](http://www.space.com/news/060628_neo_workshop.html)
16. [http://www.space.com/business technology/technology/asteroid\\_tug\\_031015.html](http://www.space.com/business technology/technology/asteroid_tug_031015.html)
17. [http://www.space.com/business technology/051109\\_asteroid\\_tractor.html](http://www.space.com/business technology/051109_asteroid_tractor.html)
18. <http://photos1.blogger.com/blogger/1933/1779/1600/CCD.jpg>

19. [http://en.wikipedia.org/wiki/Extraterrestrial\\_life](http://en.wikipedia.org/wiki/Extraterrestrial_life)
20. <http://www.spacesecurity.org/SSI2006.pdf>
21. <http://www.spacesecurity.org/publications.htm>
22. <http://www.spacesecurity.org/SSI2006ExecutiveSummary.pdf>
23. <http://www.fas.org/spp/eprint/article05.html>
24. <http://del.icio.us/DDanchev/Space>
25. <http://del.icio.us/DDanchev/SPAWAR>

422



## **Malware Search Engine (2006-07-17 23:06)**

[1]

While it seems that it takes a [2]publicly traded Internet filtering company to come up with quite some

creativity, it's always coming back to the community to break through the FUD and release a PoC [3]Malware Search Engine.

The concept is great, excluding the dark web(closed behind authentication, and basic crawler blocking approaches),

but what bothers me besides all the fuss is that it's a [4]signature based approach taking advantage of the most

recent Google's crawl of the Web. Oday malware naturally remains undetected, while it's a great way to sum up the percentage of infections with known malware on different domains/hosts, given you know what and where to look for. It's not the binary nature of a malware to emphasize on, but today's malware released under a GPL license, an issue I stated as a key factor for the [5]future growth of malware at the beginning of 2006. I also came across to an [6]article pointing out the same problem :

[7]

*" Open tools and techniques have found favor among an unlikely community. Malware writers are us-*

*ing open-source ideas and tools to share malicious code, collaborate, and wreak online mayhem, the security firm*

*McAfee said in a report issued Monday. Cyber criminals are making available source code with documentation so*

*that it can be easily modified using popular open-source project management tools like Content Versioning System*

*(CVS), thus giving malware creation a high degree of efficiency, said McAfee's Global Threat Report for 2006."*

To keep the discussion going by the time I release a summary of what I've been coming across for quite a

while – tons of bot source codes available on the public Web, barely any binaries – go through previous posts related to the diverse topic as well.

**UPDATE :** eWeek has a [8]nice article on the topic

[9]Malware

[10]Malware trends - Q1, 2006

[11]What are botnet herds up to?

[12]Why relying on virus signatures simply doesn't work anymore?

[13]Skype to control botnets?!

[14]The War against botnets and DDoS attacks

[15]Master of the Infected Puppets

[16]One bite only, at least so far!

[17]Look who's gonna cash for evaluating the maliciousness of the Web

[18]The anti virus industry's panacea - a virus recovery button

[19]No Anti Virus Software, No E-banking For You

[20]The Current State of Web Application Worms

[21]Web Application Email Harvesting Worm

[22]Unknowingly Becoming a Child Porn King

[23]Real-Time PC Zombie Statistics

[24]Malicious Web Crawling

Agobot configuration interface courtesy of Hakin9's "[25]Robot Wars – How Botnets Work".

1. <http://photos1.blogger.com/blogger/1933/1779/1600/malware.0.jpg>
  2. <http://websense.com/global/en/Investors/>
  3. <http://metasploit.com/research/misc/mwsearch/index.html>
  4. <http://metasploit.com/research/misc/mwsearch/sigs.txt>
  5. <http://www.packetstormsecurity.org/papers/general/malware-trends.pdf>
- 423
6. <http://www.redherring.com/Article.aspx?a=17610&hed=Malware+Turns+to+Open+Source&sector=Industries&subsector=Computing>
  7. [http://photos1.blogger.com/blogger/1933/1779/1600/botnet\\_rysunek\\_031128350058890.jpg](http://photos1.blogger.com/blogger/1933/1779/1600/botnet_rysunek_031128350058890.jpg)
  8. <http://www.eweek.com/article2/0,1895,1990158,00.asp>
  9. <http://del.icio.us/DDanchev/Malware>
  10. <http://ddanchev.blogspot.com/2006/02/recent-malware-developments.html>

11. <http://ddanchev.blogspot.com/2006/01/what-are-botnet-herds-up-to.html>
12. <http://ddanchev.blogspot.com/2006/01/why-relying-on-virus-signatures-simply.html>
13. <http://ddanchev.blogspot.com/2006/01/skype-to-control-botnets.html>
14. <http://ddanchev.blogspot.com/2006/02/war-against-botnets-and-ddos-attacks.html>
15. <http://ddanchev.blogspot.com/2006/02/master-of-infected-puppets.html>
16. <http://ddanchev.blogspot.com/2006/02/one-bite-only-at-least-so-far.html>
17. <http://ddanchev.blogspot.com/2006/02/look-whos-gonna-cash-for-evaluating.html>
18. <http://ddanchev.blogspot.com/2006/04/anti-virus-industrys-panacea-virus.html>
19. <http://ddanchev.blogspot.com/2006/05/no-anti-virus-software-no-e-banking.html>
20. <http://ddanchev.blogspot.com/2006/05/current-state-of-web-application-worms.html>
21. <http://ddanchev.blogspot.com/2006/06/web-application-email-harvesting-worm.html>
22. <http://ddanchev.blogspot.com/2006/06/unknowingly-becoming-child-porn-king.html>
23. <http://ddanchev.blogspot.com/2006/06/real-time-pc-zombie-statistics.html>



24. <http://ddanchev.blogspot.com/2006/06/malicious-web-crawling.html>

25. <http://www.windowsecurity.com/articles/Robot-Wars-How-Botnets-Work.html>

424



## **Open Source North Korean IMINT Reloaded (2006-07-20 23:42)**

[1]

Continuing the [2]latest coverage on [3]North Korea, and the [4]Travel Without Moving [5]series, yesterday I

came across to an ongoing initiative on [6]Google-Earthing the North Korean Military pointing out that :

*" In fact, there are several military and intelligence employees, some retired and some active, who turn the defense job into a hobby, helping to point out and explain foreign military curiosities at the very civilian level of*

*Google Earth. One current imagery analyst explained that, though he never divulges classified information, he often*

*'identifies naval vessels at' bases that ordinary Google Earth explorers have stumbled upon. Also, maps from sites*

*such as [7] Globalsecurity.org are overlayed onto the framework of Google Earth. Like an army of ants, the nearly 550,000-strong Google Earth community has voraciously explored the North Korean military installations, including :*

[8] *Musadan-ri/No-Dong missile test site*, [9] *Pipa Got naval base*, [10] *Cho Do naval base*"

Given the powerful driving force and the size of the Google Earth's community it could definitely save tax pay-

ers' dollars, but high-resolution and timely imagery still remain a critical issue here. Open Source [11]IMINT is gaining scale and I'm sure [12]someone's watching the trend as well.

### **Related resources and posts :**

[13]GEOINT

[14]Reconnaissance

[15]The "threat" by Google Earth has just vanished in the air

[16]Suri Pluma - a satellite image processing tool and visualizer

[17]Security quotes : a FSB (successor to the KGB) analyst on Google Earth

[18]Satellite Reconnaissance of the Future (1998)

[19]Military Reconnaissance Satellites (IMINT)

[20]Military Intelligence Satellites

[21]North Korea Sightseeing

[22]Shedding light on North Korea (330+ placemarks)

1.

<http://photos1.blogger.com/blogger/1933/1779/1600/goods>

[ubs.jpg](#)

2. <http://ddanchev.blogspot.com/2006/06/north-korea-turn-on-lights-please.html>
3. <http://ddanchev.blogspot.com/2006/07/north-koreas-cyber-warfare-unit-121.html>
4. <http://ddanchev.blogspot.com/2006/07/travel-without-moving-north-korea.html>
5. [http://ddanchev.blogspot.com/2006/05/travel-without-moving-korean\\_27.html](http://ddanchev.blogspot.com/2006/05/travel-without-moving-korean_27.html)
6. <http://www.radioopensource.org/google-earthing-the-north-korean-military/>
7. [http://www.globalsecurity.org/wmd/world/dprk/no\\_dong\\_imagery.htm](http://www.globalsecurity.org/wmd/world/dprk/no_dong_imagery.htm)
8. <http://bbs.keyhole.com/ubb/download.php?Number=213366>
9. <http://bbs.keyhole.com/ubb/download.php?Number=487653>
10. <http://bbs.keyhole.com/ubb/download.php?Number=507504>
11. <http://www.fas.org/irp/imint/index.html>
12. <http://www.nro.gov/>
13. <http://del.icio.us/DDanchev/GEOINT>
14. <http://del.icio.us/DDanchev/Reconnaissance>

15. <http://ddanchev.blogspot.com/2006/04/threat-by-google-earth-has-just.html>
16. <http://ddanchev.blogspot.com/2006/02/suri-pluma-satellite-image-processing.html>
17. <http://ddanchev.blogspot.com/2006/01/security-quotes-fsb-successor-to-kgb.html>
18. [http://www.dtic.mil/doctrine/jel/jfq\\_pubs/0718.pdf](http://www.dtic.mil/doctrine/jel/jfq_pubs/0718.pdf)
19. <http://www.cdi.org/terrorism/satellites.cfm>
20. [http://rst.gsfc.nasa.gov/Intro/Part2\\_26e.html](http://rst.gsfc.nasa.gov/Intro/Part2_26e.html)
21. <http://www.googleearthhacks.com/downloads/country.php?country=76>
22. <http://bbs.keyhole.com/ubb/showflat.php?Number=145735>

425

426



## **Budget Allocation Myopia and Prioritizing Your Expenditures (2006-07-21 00:43)**

[1]

Top management's empowerment - the dream of every CSO, or IT manager responsible for allocating the

infosec budget, and requesting future increases. The biggest downside of your current or future empowerment, is

how easy it is to get lost in a budget allocating myopia compared to actual prioritizing of your expenditures. According to Gartner, [2]security is all about percentage of budget allocation :

*" Organizations that have reached a high level of IT security practice maturity can safely reduce spending to between 3 % and 4 % of the IT budget by 2008, according to research firm Gartner Inc. By contrast, organizations that*

*are inefficient or have historically under invested in security may spend upwards of 8 % of their IT budget on security.*

*This means that many organizations will still be investing aggressively for the next few years. Rich Mogull, research vice president and conference chair of the Gartner IT Security Summit which starts in Sydney Tuesday, said that there are now solutions to most information security problems. It's just a matter of implementing the technology efficiently and effectively so resources can be focused on new threats," Mogull said. While information security has become a highly specialized branch of IT, commodity security functions are often being returned to IT operations. Organizations that are still impacted by everyday, routine threats must ramp up and become more mature in their approach. "*

I find this a wrong emphasis on higher spending as the corner stone of "better security", and even if it is so, who's your benchmark at the bottom line? In a previous in-depth post on [3]Valuing Security and Prioritizing Your

Expenditures, I discussed the currently hard to implement ROSI model, and pointed out the following key points on

data security breaches and security investments :

- on the majority of occasions companies are taking an outdated approach towards security, that is still living in the perimeter based security solutions world
- companies and data brokers/aggregators are often reluctant to report security breaches even when they have the legal obligation to do so due to the fact that, either the breach still hasn't been detected, or the lack of awareness on

what is a breach worth reporting

- the flawed approaches towards quantifying the costs related to Cybercrime are resulting in overhyped statements in direct contradiction with security spending

- companies still believe in the myth that spending more on security, means better security, but that's not al-

ways the case

- given the flood of marketing and the never ending "media echo" effect, decision makers often find them-

selves living with current trends, not with the emerging ones, which is what they should pay attention to

There's also a rather simplistic explanation on the effect of industry convergence :

*" Mogull also said that functional convergence in security products is occurring.*

*For example, host firewalls,*

*antivirus, antis spam, and basic host intrusion prevention are combining into single, desktop agents. In the future, this will make security less complex, he said. "*

Wish the analyst has reached the potential TCO increase and the beneficial diversification of appliances/products

trade-off concept stage, one that naturally depends on the perspective of course. Meanwhile, here's [4]an article on

how NOT to "sell security" to your CEO, they tend to understand the basics of ROI, it's just the RO(S)I they want to scientifically apply - compliance is perhaps your best friend these days. It's not about the percentage of spending, but on what you're actually spending for, and when.

427

Go through a previous post on [5]information security market trends to consider, and try to stay on the top of security, not in line with it.

1.

<http://photos1.blogger.com/blogger/1933/1779/1600/market.jpg>

2. [http://computerworld.com/action/article.do?](http://computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=security&articleId=9001831)

[command=viewArticleBasic&taxonomyName=security&articleId=9001831](http://computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=security&articleId=9001831)

[&taxonomyId=17](http://computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=security&articleId=9001831)

3. <http://ddanchev.blogspot.com/2006/05/valuing-security-and-prioritizing-your.html>

4. [http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=112203&source=NLT\\_SHARK&n](http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=112203&source=NLT_SHARK&n)

[lid=6](#)

5. <http://ddanchev.blogspot.com/2006/04/spotting-valuable-investments-in.html>

428



## **When Financial and Information Security Risks are Supposed to Intersect (2006-07-21 01:30)**

[1]

Interesting [2]security event at Morgan Stanley's NYC headquarters related to insider abuse, mostly interesting

because the clients' list and charged fees weren't even uploaded on any removable media, but **forwarded to the**

**consultant's private email account :**

*" A former consultant to Morgan Stanley has been arrested and charged with stealing an electronic list of hedge funds and the rates the investment bank charges them. The hedge funds are clients in the company's prime brokerage*

*business. According to court documents, Chilowitz is accused of sending a copy of the firm's administrative client list and its client rate list for the prime brokerage business in February from Morgan Stanley's offices in New York to his personal e-mail account at his home in Virginia. "*



I once said that nothing's impossible, the impossible just takes a little while, but given [3]who Morgan Stanley

is when it comes to risk management, assessment, let's don't say risk engineering - psst, [4]paying \$15m in order not

to pay \$1.5B is such a sound investment - they should have never allowed for this type of info to leave over the Web.

Meanwhile, the WSJ is reporting that [5]Employers Increasingly Firing Staffers for E-mail Violations :

*" The news comes from the [6] 2006 Workplace E-Mail, Instant Messaging and Blog survey from the American Management Association and the ePolicy Institute, according to the Journal. The survey found that more than a*

*quarter of the employers queried had fired an employee for violating company e-mail policy, up 9 percent from the*

*17 percent of employers who let employees go for similar violations in 2001, the Journal reports. On top of this*

*finding, the survey also said that 2 percent of respondents had fired workers for instant-message correspondences*

*that weren't appropriate, and another 2 percent of employers said they'd fired a staffer for posting distasteful content on a Web log—or blog—be it their professional or personal page, according to the Journal. "*

[7]Security policies are not the panacea of security, they are the basics, so consider developing and monitor-

ing the effectiveness of one. My advise - think twice before feeling like a smart ass for exploiting your interns next

time, and yes, [8]fingerprint [9]your most [10]valuable [11]IP assets as well.

429

1. <http://photos1.blogger.com/blogger/1933/1779/1600/morgan-stanley-NYC.jpg>
2. <http://news.moneycentral.msn.com/provider/providerarticle.asp?feed=AP&Date=20060717&ID=5870774>
3. [http://en.wikipedia.org/wiki/Morgan\\_Stanley](http://en.wikipedia.org/wiki/Morgan_Stanley)
4. <http://ddanchev.blogspot.com/2006/02/smoking-emails.html>
5. [http://www.cio.com/blog\\_view.html?CID=23047](http://www.cio.com/blog_view.html?CID=23047)
6. [http://www.amanet.org/press/amanews/2006/blogs\\_2006.htm](http://www.amanet.org/press/amanews/2006/blogs_2006.htm)
7. <http://www.windowsecurity.com/pages/security-policy.pdf>
8. <http://www.vontu.com/products/competitive.asp>
9. <http://www.tablus.com/page.php?id=137>
10. <http://www.reconnex.net/products/default.asp>
11. <http://www.vericept.com/solutions/intellectual.asp>

430



## Anti Virus Signatures Update - It Could Wait (2006-07-21 02:07)

[1]

It's a common myth that all AV vendors exchange the malware they come across in between themselves, whereas

that's obviously not always the case. And even if they don't, you'd better achieve a higher state of security in respect to ensuring your PC or network are protected from the majority of **known malware threats**, trouble is the average

end users whose Internet connection speed is reaching that of an average ISP (metaphor), doesn't seem to bother

because of the following concerns :

- it could wait
- it takes decades to update
- it would influence their superman's productivity
- where's the update button by the way?

From the press release of a [2]commissioned survey :

*" Harris Interactive® fielded the online survey among a nationwide sample of 2,079 U.S. adult computer users*

*18 years of age or older. The survey reveals that: Despite 55 percent being very confident or confident in the protection offered by the antivirus program on their computer, 42 percent have been affected by malware. A surprising 65*

*percent have postponed updating their virus protection. Of these adults, their top reasons for not updating are:*

*It was too disruptive to what they were doing on the computer - **38 %***

*They thought it was something that could wait - **32 %***

*They thought it would take too long - **27 %***

*They weren't sure how to update the antivirus program - **14 %***

These very same end users represent among the key factors for successful assembling of botnets these days.

If you secure the entire population, you'll end up with a secure sample itself, but the novice user's lack of incentives is ruining the whole effect - and driving the [3]DDoS protection tools market segment of course. I also wonder how

did [4]Gartner manage to estimate Panda Software's revenues and market share, given that compared to the rest of

the publicly traded companies it's free from the burden of having stakeholders breathing down their neck?

Failures in Detection courtesy of [5]VirusTotal.

431

1. [http://photos1.blogger.com/blogger/1933/1779/1600/signatures\\_sharing.jpg](http://photos1.blogger.com/blogger/1933/1779/1600/signatures_sharing.jpg)

2. <http://www.eset.com/company/article.php?contentID=1553>

3. <http://ddanchev.blogspot.com/2006/02/war-against-botnets-and-ddos-attacks.html>

4. [http://www.gartner.com/press\\_releases/asset\\_154006\\_11.html](http://www.gartner.com/press_releases/asset_154006_11.html)

5. <http://www.virustotal.com/>

432



## **Detailed Penetration Testing Framework (2006-07-21 02:44)**

[1]

This framework is simply amazing, as it takes you through [2]the entire process of penetration testing, step-

by-step in between references to the tools necessary to conduct a test – wish experience was commodity as well.

[3]Best practices are prone to evolve the way experience does, so consider adding some of your know-how, and going

through Fyodor's [4]Top 100 Network Security Tools list in case you're looking for improved efficiency. It's not about

the quality and diversity of tools, but about the quality of the approach, still the framework is a nice one to begin with.

Photo courtesy of IBM, featuring ethical hacker [5]Nick Simicich. You may also find Secure DVD, a collection

of the 10 Best Security Live CD Distros (Pen-Test, Forensics & Recovery) [6]handy.

1. <http://photos1.blogger.com/blogger/1933/1779/1600/Dcp00533-784234.jpg>
2. <http://www.vulnerabilityassessment.co.uk/Penetration%20Test.html>
3. <http://www.isecom.org/osstmm/>
4. <http://sectools.org/>
5. <http://www.cnn.com/TECH/computing/9811/27/hacker.interview/>
6. <http://www.securedvd.org/about.html>

433



## **Searching for Source Code Security Vulnerabilities (2006-07-21 16:36)**

[1]

While Google was quick enough to censor the colourful  
[2]Malware Search [3]logo - colourful branding -

here's another recently started initiative, [4]Bugle - a  
google based source code bug finder :

*" Bugle is a collection of search queries which can help to identify software security bugs in source code available on the web. The list at the moment is rather small (you get the idea though), hopefully people will start sending more queries. Source code review is not a straight forward*

*operation , using the list you will get pinpoints and not definite results. "*

It could easily help you spot source code containing common bugs without the need of [5]using a scientific model to predict vulnerabilities, but you should also consider the [6]powerful source code search engine Koders which is **currently searching 225,816,744 lines of code**, and [7]provides you with the option to segment your queries based on programming language.

### **Related resources:**

[8]SecureProgramming.com - latest update January, 2005, useful links through

[9]An overview of common programming security vulnerabilities and possible solutions

[10]Insecure Programming by example

[11]Top 7 PHP Security Blunders

1. <http://photos1.blogger.com/blogger/1933/1779/1600/bugle.jpg>

2. <http://ddanchev.blogspot.com/2006/07/malware-search-engine.html>

3. <http://metasploit.com/research/misc/mwsearch/malware.jpg>

4. <http://www.cipher.org.uk/index.php?p=projects/bugle.project>

5. <http://ddanchev.blogspot.com/2006/07/scientifically-predicting-software.html>
6. <http://koders.com/>
7. <http://koders.com/info.aspx?c=GettingStarted>
8. <http://www.secureprogramming.com/>
9. <http://fort-knox.org/thesis.pdf>
10. <http://community.core-sdi.com/~gera/InsecureProgramming/>
11. <http://www.sitepoint.com/print/php-security-blunders>

434



## **An Intergalactic Security Statement (2006-07-24 22:44)**

[1]

Hell of a comment on the [2]Malware Search Engine.  
[3]Hackers crack secret Google malware search codes :

*" Hidden malware search capabilities within Google which were reserved for antivirus and security research*

*firms just weeks ago have been cracked by hackers, according to security industry sources. The key to finding malware in Google lies in having the signature for the specific malware program, according to researchers from enterprise IT*



*security firm Secure Computing. However, the company reported that these previously hidden search capabilities have recently fallen into the hands of hackers. Why bother creating a new virus, worm or Trojan when you can simply find one and download it using Google? said Paul Henry, vice president of strategic accounts at Secure Computing.*

*Unskilled hackers can use this previously unknown capability of Google to download malware and release it on the*

*internet in targeted attacks as if they wrote it themselves. "*

Bothering to create a new piece of malware and ensuring its payload gets regularly updated to avoid AV de-

tection is perhaps the most logical need compared to doing reconnaissance for known malware through Google.

Looking for the signature means the piece of malware has already been detected somehow, somewhere, namely it's

useless even to a script kiddie as I doubt one would do a favor to another, thus increasing the size of someone else's

botnet. What you can actually use it for, is look for [4]packed binary patterns, or [5]known functions, and draw up

better conclusions.

I really hope Secure Computing are more into [6]harnessing the brand and product portfolio's power of Ci-

pherTrust, than they are into the [7]dangers of known malware, not that there aren't exceptions of course!

Space wisdom courtesy of [8]Doctor Fun.

1. <http://photos1.blogger.com/blogger/1933/1779/1600/df941012.0.jpg>
2. <http://ddanchev.blogspot.com/2006/07/malware-search-engine.html>
3. <http://www.vnunet.com/vnunet/news/2160908/hackers-crack-secret-google>
4. <http://blogs.securiteam.com/index.php/archives/513>
5. <http://asert.arbornetworks.com/2006/07/googling-for-malware-bobbing-for-mass-mailers/>
6. <http://www.redherring.com/article.aspx?a=17587>
7. <http://ddanchev.blogspot.com/2006/07/anti-virus-signatures-update-it-could.html>
8. <http://www.ibiblio.org/Dave/>

435



## **Latest Report on Click Fraud (2006-07-25 00:09)**

[1]

Google does have countless features, and it's not even considering to stop rolling new ones, but the secret

to its huge [2]market capitalization and revenue stream remains its advertising model fully utilizing the [3]Long

tail's concept. Therefore, click fraud remains the key issue to deal with, if they want to [4]continue beating Wall Street's

expectations. Last week [5]Google released [6]a commissioned report evaluating their anti click fraud methods,

here's an excerpt on the four lines of defense :

" Google has built the following four 'lines of defense' for detecting invalid clicks: **pre-filtering, online filtering,**

**automated offline detection and manual offline detection**, in that order. Google deploys different detection methods in each of these stages: the rule-based and anomaly-based approaches in the pre-filtering and the filtering

stages, the combination of all the three approaches in the automated offline detection stage, and the anomaly-based

approach in the offline manual inspection stage. This deployment of different methods in different stages gives

Google an opportunity to detect invalid clicks using alternative techniques and thus increases their chances of

detecting more invalid clicks in one of these stages, preferably proactively in the early stages. "

Despite Eric Schmidt's comments on [7]click fraud as "self correcting" issue, [8]Mark Cuban takes another per-

spective I find a very relevant one. The key remains the balance between Google's technologies and efforts to build

awareness on the problem, very informative report. Pay-per-click is a powerful model forwarding the responsibility

for eventual transactions to the advertiser's value added proposition, as compared to a [9]Pay per action model. I

doubt Google would have ever reached [10]a stock split debate in its history if it were to use one.

Moreover, with the growing interest in a [11]Pay-per-call model and the [12]rise in [13]voice phishing, it turns

the trend into a hot one to keep an eye on for the upcoming future.

1.

[http://photos1.blogger.com/blogger/1933/1779/1600/click\\_click.jpg](http://photos1.blogger.com/blogger/1933/1779/1600/click_click.jpg)

2. <http://finance.google.com/finance?q=google>

3. [http://en.wikipedia.org/wiki/Long\\_tail](http://en.wikipedia.org/wiki/Long_tail)

4.

<http://www.marketwatch.com/News/Story/Story.aspx?dist=newsfinder&siteid=google&guid=%7B635681E2-7667-49FC>

<http://www.marketwatch.com/News/Story/Story.aspx?dist=newsfinder&siteid=google&guid=%7B635681E2-7667-49FC-A7BB-F4C44A0582F5%7D&keyword=>

5. [http://googleblog.blogspot.com/pdf/Tuzhilin\\_Report.pdf](http://googleblog.blogspot.com/pdf/Tuzhilin_Report.pdf)

6. <http://googleblog.blogspot.com/2006/07/findings-on-invalid-clicks.html>

7. <http://blog.searchenginewatch.com/blog/060710-080753>

8. <http://www.blogmaverick.com/entry/1234000470073786/>
9. <http://battellemedia.com/archives/002662.php>
10. [http://news.com.com/2061-11199\\_3-6022011.html](http://news.com.com/2061-11199_3-6022011.html)
11. <http://www.ingenio.com/>
12. [http://www.theregister.co.uk/2006/06/26/voice\\_phishing/](http://www.theregister.co.uk/2006/06/26/voice_phishing/)
13. <http://www.websense.com/securitylabs/alerts/alert.php?AlertID=534>

436



## **Splitting a Botnet's Bandwidth Capacity (2006-07-26 20:29)**

[1]

Metaphorically speaking, I always say that the massess of end users' bandwidth is reaching that of a mid

size ISP, while the lack of incentives or plain simple awarenss is resulting in today's easily assembled botnets. Freaky perspective, but that's what I perceive the trade-off out of this [2]major economic boost given the improved connectivity [3]France Telecom is about to offer to its customers in 2007/2008 - [4]Fiber at Home with **2.5Gbits/s download**, and **1.2Gbits/s upload**. As it looks like, an end user is gonna be worth a hundred more infected ones in the near future.

[5]More on malware.

1.

[http://photos1.blogger.com/blogger/1933/1779/1600/zombie\\_puppets.jpg](http://photos1.blogger.com/blogger/1933/1779/1600/zombie_puppets.jpg)

2.

[http://www.oecd.org/document/26/0,2340,en\\_2649\\_34255\\_16220890\\_1\\_1\\_1\\_1,00.html](http://www.oecd.org/document/26/0,2340,en_2649_34255_16220890_1_1_1_1,00.html)

3.

<http://translate.google.com/translate?u=http%3A%2F%2Fwww.presence-pc.com%2Factualite%2Fftth-experience-18331%2F&langpair=fr%7Cen&hl=en&ie=UTF8>

4. <http://slashdot.org/articles/06/07/26/127205.shtml>

5. <http://ddanchev.blogspot.com/2006/07/malware-search-engine.html>

437



## **The Beauty of the Surrealistic Spam Art (2006-07-27 02:03)**

[1]

Given the volume of spam representing over 50 % of the world's email traffic, obviously to some it represents

a huge sample to draw sadness or anger out of, and of course, visualize the findings. [2]One man's spam is Alex

Dragulescu's art :

*" He doesn't use Photoshop but simply writes code to create computer art. For the [3]Spam Plants, he parsed*

*the data within junk e-mail—including subject lines, headers and footers—to detect relationships between that data.*

*Then he visually represents those relationships. For example, the program draws on the numeric address of an e-mail*

*sender and matches those numbers to a color chart, from 0 to 225. It needs three numbers to define a color, such*

*as teal, so the program breaks down the IP address to three numbers so it can determine the color of the plant. The*

*time a message is sent also plays a role. If it's sent in the early morning, the plant is smaller, or the time might stunt the plant's ability to grow, Dragulescu said. The size of the message might determine how bushy the plant is. Certain keywords, such as "Nigerian," might trigger more branches. But Dragulescu did not inject any irony. **Messages about***

***Viagra do not grow taller, for example. "***

I feel that now every spammer can pretend about being a stylish art admirer, with his spamming historical

performance hanging on the wall, or perhaps it's my surrealistic black humor.

### **Related posts on spam and visualization :**

[4]Fighting Internet's email junk through licensing

[5]An Over-performing Spammer

[6]Consolidation, or Startups Popping out Like Mushrooms?

[7]Dealing with Spam - The O'Reilly.com Way

[8]Visualization, Intelligence and the Starlight project

[9]Visualization in the Security and New Media world

1.

[http://photos1.blogger.com/blogger/1933/1779/1600/spam\\_plants.0.jpg](http://photos1.blogger.com/blogger/1933/1779/1600/spam_plants.0.jpg)

2.

[http://news.com.com/One+mans+spam+is+anothers+art/2100-1025\\_3-6098479.html](http://news.com.com/One+mans+spam+is+anothers+art/2100-1025_3-6098479.html)

3. <http://www.sq.ro/spamplants.php>

4. <http://ddanchev.blogspot.com/2006/04/fighting-internets-email-junk-through.html>

5. <http://ddanchev.blogspot.com/2006/06/over-performing-spammer.html>

6. <http://ddanchev.blogspot.com/2006/06/consolidation-or-startups-popping-out.html>

7. <http://ddanchev.blogspot.com/2006/06/dealing-with-spam-oreillycom-way.html>

8. <http://ddanchev.blogspot.com/2006/01/visualization-intelligence-and.html>

9. <http://ddanchev.blogspot.com/2006/03/visualization-in-security-and-new.html>

438





## **DVD of the Weekend - Path to War (2006-07-30 23:00)**

[1]

As I've been busy catching up with way too many things to list them, I'd better finalize my creativity efforts

and provide you with the results as they appear during the week. Meanwhile, current events being constantly

streamed and brainwashed from every TV channel you try to watch - remember how in [2]1984 only the party

leaders had the privilege to turn off their 24/7 propaganda streams? Feel empowered nowadays - made me think

on how today's situation slightly represents the one filmed in the [3]Path to War, especially the partisan warfare

activities. You can never win a partisan war, what you'll end up with is your ego and nose bleeding, and your heroic

wings sort of broken. Feeling, or positioning yourself for powerful PSYOPS while destroying a country's infrastructure

to eradicate the partisan fighters, is one of my favorite moments in the movie, especially when they realized how

they've **managed to destroy 140 % of Vietnam's infrastructure and were still losing the war.**

Even worse, having to power and diplomatic influence to make a change, while being a bureaucrat to win

time as someone else's about to take care of your dirty laundry is such a bad example for the rest of the democratic

world, yet a convenient one.

Great post at DefenseTech on [4]autonomous warfare, destroy the oil resources to limit the movement of sup-

pliers - have [5]a dozen of grannies move them on bicycles or take it personally, destroy a bridge, and see a wooden

one build within day or two, every war is an act of terrorism by itself, where the term "acceptable levels of casualties"

constantly jumps from the military to the political dictionary.

### **Previous DVDs of the Weekend and related comments:**

[6]DVD of the Weekend - The Lone Gunmen

[7]DVD of the Weekend - The Outer Limits - Sex And Science Fiction Collection

[8]DVD of the Weekend - War Games

[9]DVD of the Weekend - The Immortals

[10]DVD of the Weekend - Lawnmower man - Beyond Cyberspace

1. <http://photos1.blogger.com/blogger/1933/1779/1600/B00006LSH3.02.LZZZZZZZ.jpg>

2. <http://www.imdb.com/title/tt0087803/>

3. <http://www.imdb.com/title/tt0218505/>

4. <http://www.defensetech.org/archives/002618.html>

5.

[http://www.emergentchaos.com/archives/2006/07/why\\_profiling\\_doesnt\\_work.html](http://www.emergentchaos.com/archives/2006/07/why_profiling_doesnt_work.html)

6. <http://ddanchev.blogspot.com/2006/02/dvd-of-weekend-lone-gunmen.html>

7. <http://ddanchev.blogspot.com/2006/02/dvd-of-weekend-outer-limits-sex-and.html>

8. <http://ddanchev.blogspot.com/2006/03/dvd-of-weekend-war-games.html>

9. <http://ddanchev.blogspot.com/2006/03/dvd-of-weekend-immortals.html>

10. <http://ddanchev.blogspot.com/2006/03/dvd-of-past-weekend.html>

439

x



## **Japan's Reliance on U.S Spy Satellites and Early Warning Missile Systems (2006-07-31 02:14)**

[1]

With China breathing down Japan's neck, and North Korea crying for attention by actively experimenting

with [2]symmetric and [3]asymmetric warfare capabilities, Japan's need for better reconnaissance, and limiting of

its imagery gathering dependence has been in the execution stage for years as [4]Reliance on U.S. intelligence

on

missile launch shows need for improvement :

*" The two spy satellites currently in operation are both polar orbiters circling the globe at altitudes of 400 to 600 kilometers. If the fourth, a SAR satellite, is launched in 2007 as planned, it will complete the four-satellite*

*reconnaissance system, and the country will be able to monitor any point on Earth at least once a day, officials*

*said. It will therefore become possible for Japan to monitor day-to-day changes in North Korean missile-launching*

*sites. The problem, however, is if the system will be effective at the moment of a missile launch, which would*

*depend on the weather and positions of the satellites at the time, officials said on condition of anonymity. In stark contrast with Japan, the United States has orbited more than 100 satellites, at least 15 of which are reportedly for intelligence-gathering purposes, they said. As experts put it, the U.S. satellites can identify objects as small as 8 to 9*

*centimeters in size if weather conditions are ideal. The United States has five early-warning satellites, including one for backup purposes, keeping watch over North Korea around the clock, they said. "*

[5]

They're definitely using open source [6]IMINT on North Korea as well, or requesting detailed imagery on demand

through [7]commercial providers, in between further developing their [8]early warning [9]systems. Go through

an

440

article on [10]Japan's Information Gathering Satellites Imagery Intelligence in case you're interested in their past efforts in this direction. However, I feel it's their neighbors' [11]cyber warfare capabilities they should be also worried about.

Image courtesy of Northrop Grumman.

1.

[http://photos1.blogger.com/blogger/1933/1779/1600/corona\\_first\\_spy\\_satellite.2.jpg](http://photos1.blogger.com/blogger/1933/1779/1600/corona_first_spy_satellite.2.jpg)

2. <http://ddanchev.blogspot.com/2006/07/travel-without-moving-north-korea.html>

3. <http://ddanchev.blogspot.com/2006/07/north-koreas-cyber-warfare-unit-121.html>

4.

<http://www.yomiuri.co.jp/dy/national/20060731TDY03003.htm>

5.

[http://photos1.blogger.com/blogger/1933/1779/1600/testbed\\_hr.jpg](http://photos1.blogger.com/blogger/1933/1779/1600/testbed_hr.jpg)

6. <http://ddanchev.blogspot.com/2006/07/open-source-north-korean-imint.html>

7. <http://www.lockheedmartin.com/wms/findPage.do?dsp=fec&ci=13088&rsbci=12975&fti=0&ti=0&sc=400>

8. <http://www.lockheedmartin.com/wms/findPage.do?dsp=fec&ci=13169&rsbci=12975&fti=0&ti=0&sc=400>

9. [http://www.northropgrumman.com/missiledefense/About\\_MD.html](http://www.northropgrumman.com/missiledefense/About_MD.html)

10. <http://www.fas.org/spp/guide/japan/military/imint/index.html>

11. <http://ddanchev.blogspot.com/2006/05/whos-who-in-cyber-warfare.html>

441



## **Things Money Cannot Buy (2006-07-31 21:42)**

[1]

1. **Love** with tingles

2. True **Friends**

3. **Respect**, one when the results go beyond the position and size of market capitalization

4. **Style**

5. **Childhood** full of joy

6. **Knowledge**, diploma and insider leaks are something else

7. And obviously **Innovation** as you can see at this slide and compare it to the rough reality for [2]the top tech R &D

spenders. 800 pound market capitalization gorillas for sure, but not innovators. A knowledge driven society results

in [3]talent wars – [4]permanently attracting the walking case studies is also important.

Outspending ends up in [5]budget allocation myopia, compared to actually prioritizing your R &D efforts. You

aren't productive when you have all the cash in the world, exactly the opposite, and passion does play a crucial role

when it comes to creativity. Go through a handy summary of a study on [6]Does R &D spending deliver results? as

well.

1.

[http://photos1.blogger.com/blogger/1933/1779/1600/RD\\_spending.jpg](http://photos1.blogger.com/blogger/1933/1779/1600/RD_spending.jpg)

2.

[http://paul.kedrosky.com/archives/2006/07/28/microsofts\\_anti.html](http://paul.kedrosky.com/archives/2006/07/28/microsofts_anti.html)

3.

<http://www.forbes.com/columnists/columnists/forbes/2005/1031/045.html>

4.

[http://en.wikipedia.org/wiki/Science\\_and\\_technology\\_in\\_the\\_United\\_States#Science\\_immigration](http://en.wikipedia.org/wiki/Science_and_technology_in_the_United_States#Science_immigration)

5. <http://ddanchev.blogspot.com/2006/07/budget-allocation-myopia-and.html>

6. [http://www.businessweek.com/the\\_thread/techbeat/archives/2005/10/does\\_rd\\_spendin.html](http://www.businessweek.com/the_thread/techbeat/archives/2005/10/does_rd_spendin.html)

442

**2.8**

**August**

443



x

## **But Of Course It's a Pleasant Transaction (2006-08-02 15:02)**

[1]

Great example of [2]automated bots attacking Ebay's core trust establishing process- the feedbacks provided

by users taking advantage of [3]the wisdom of crowds to judge on their truthfulness :

*" Again, a sharp eye may notice that feedback comments received from sellers are identical, and read almost*

*in the same order.*

*This is because most 1-cent-plus-no-delivery-cost sellers automate the whole transaction:*

*should someone buy their eBooks for one cent each, some scripts email it automatically to the buyer, and leaves a*

*standard feedback comment on the buyer's profile. So, if we recollect everything, the following is probably happening: 1. Someone is massively creating randomly named, fake user accounts (probably in a more or less automated*

*fashion).*

*2. Those fake users, powered by automated web spider software, are set to scavenge eBay for 1-cent "buy it now"*

*items and buy them.*

*3. Automatically, the 1-cent item seller script is emailing the buyer with the item, and posts its standard feedback on his profile.*

*4. The fake user automatically responds with a standard feedback comment on the seller's profile.*

*In a nutshell: Two bots are talking. And doing business. "*

The use of CAPTCHAs, and ensuring the bots never manage to register themselves, is as important as the au-

tomated [4]the process of bypassing CAPTCHA authentication . Expect to see a much better random generation of

pseudo users, and their feedbacks compared to these one. And since [5]Ebay is no longer an intermediary, but a

platform, bots got plenty of seed data to begin their life with, don't they?

These very same techniques apply to common networks such as the Internet Relay Chat, and the majority of

instant messengers where malware tries to, either take advantage of a momentum and forward itself to a buddy, or

keep the discussion going until the time for a fancy photo session exchange has come.

1.  
<http://photos1.blogger.com/blogger/1933/1779/1600/sellerprofileck1.jpg>

2.  
[http://www.fortinet.com/FortiGuardCenter/reports/roundup\\_j](http://www.fortinet.com/FortiGuardCenter/reports/roundup_j)

[uly\\_2006.html](#)

3. [http://en.wikipedia.org/wiki/The\\_Wisdom\\_of\\_Crowds](http://en.wikipedia.org/wiki/The_Wisdom_of_Crowds)

4. <http://sam.zoy.org/pwntcha/>

5. <http://developer.ebay.com/>

444



**One Time Password Generating Credit Card (2006-08-03 01:39)**

[1]

This is cute as it solves a major problem with customers having to use, and more easily lose tokens. Neat integration with the push of a button on the [2]one time password generating credit card :

*" It took InCard four years to develop the card, Finkelstein said. The company combined technology from a Tai-*

*wanese display maker, a U.S. battery manufacturer and a French security team, he said. A Swiss partner, NagraID,*

*owns the rights to the process to combine the pieces and actually manufacture the technical innards of the card. The biggest development challenges were the ability to bend the card, power consumption and thickness, Finkelstein said.*

*The result is a card that's as thin and flexible as a regular credit card and is guaranteed to work for three years and 16,000 uses. "Which is about 15 times a day, seven days a week," Finkelstein said. "*

Compliance with the FFIEC, or an emerging trend of convergence, trouble is it doesn't solve the majority of

issues related to phishing attacks, rather it has the potential to undermine other companies' offerings. Now all they

need is someone who'll take the role of an evangelist besides the well networked company executives.

### **Related posts:**

[3]Anti Phishing Toolbars - Can You Trust Them?

[4]Heading in the Opposite Direction

[5]No Anti Virus Software, No E-banking for You

445

1.

[http://photos1.blogger.com/blogger/1933/1779/1600/credit\\_card\\_authentication.jpg](http://photos1.blogger.com/blogger/1933/1779/1600/credit_card_authentication.jpg)

2.

[http://news.com.com/A+password+for+your+credit+cards/2100-1029\\_3-6101121.html](http://news.com.com/A+password+for+your+credit+cards/2100-1029_3-6101121.html)

3. <http://ddanchev.blogspot.com/2006/03/anti-phishing-toolbars-can-you-trust.html>

4. <http://ddanchev.blogspot.com/2006/04/heading-in-opposite-direction.html>

5. <http://ddanchev.blogspot.com/2006/05/no-anti-virus-software-no-e-banking.html>

446

x

## **Achieving Information Warfare Dominance Back in 1962 (2006-08-03 19:36)**

[1]

The point here isn't [2]the consolidation indicated in the article :

*" The consolidation involves Singer's headquarters staff, and subordinate Naval Security Group Activities (NSGA) and detachments (NSGD). When fully completed, the action will combine the Navy's enlisted Cryptologic Technicians*

*and Information Warfare officers into the same organization as the Navy's Information Systems Technicians and*

*Information Professional officers. The IO warfare area is composed of five core integrated capabilities: Electronic*

*Warfare, Computer Network Operations, Psychological Operations, Military Deception and Operational Security.*

*These combine with related capabilities to provide "Information Dominance," the concept of controlling an adversary's use of the information and communications environment while protecting one's own. "*

but the advances of intercepting electromagnetic emissions reflected off the Moon back in 1962, through the

### **NRRO 600-Foot Steerable Parabolic Antenna :**

*" Naval Radio Research Observatory (NRRO). This observatory is to be erected at [3] Sugar Grove, West Virginia for exploiting lunar reflective techniques for the purposes of intelligence collection, radio astronomy, and*

*communications-electronics research. A 600-foot steerable parabolic radio antenna will provide for the reception of*

*electromagnetic emissions reflected off the moon. As an intelligence device it will provide for reception and analyzing emissions from areas of the world not now accessible by any other known method, short of physical penetration. The*

*Observatory is planned to be operational in FY 1962. "*

Here's [4]more info on the [5]concept :

*" Although the 600-ft telescope was never built, a satellite-based alternative, called '[6]GRAB' ([7]Galactic RAdi-ation Background), was launched in June of 1960. Again, this was a dual-use system. The world's first elint satellite and astronomical observatory were integrated into the same satellite bus, with astronomy serving as an operational*

*front for the whole. A second GRAB was launched in 1962. This interface of classified and basic research tells us*

*about the pursuit of science and science-based technologies during the Cold War. "*

Nowadays it just seems to be full of bird listeners using parabolic microphones, [8]activists "hacking" TV and Radio signals, and others conducting sophisticated [9]TECHINT on the war field.

### **Related resources:**

[10]InformationWarfare

[11]Cyber Warfare

[12]PSYOPS

[13]Intelligence

1.

<http://photos1.blogger.com/blogger/1933/1779/1600/sugargrove.jpg>

2. <http://cryptome.org/echelon-reorg.htm>

3. <http://eyeball-series.org/sugar-eyeball.htm>

4. <http://sss.sagepub.com/cgi/content/abstract/31/2/207>

5. <http://www.gb.nrao.edu/~rcreager/GBTMetrology/documentation/gbtmemo/gbtmemo166.html>
6. <http://www.fas.org/spp/military/program/sigint/grab.htm>
7. <http://www.military.com/Resources/ResourceFileView/GRAB.htm>
8. <http://www.naharnet.com/domino/tn/NewsDesk.nsf/0/236DD3CF2B77BB52C22571BD006DB6EC?OpenDocument>
9. [http://www.fas.org/blog/secretcy/2006/07/dod\\_manual\\_on\\_technical\\_intell.html](http://www.fas.org/blog/secretcy/2006/07/dod_manual_on_technical_intell.html)
10. <http://del.icio.us/DDanchev/InformationWarfare>
11. <http://del.icio.us/DDanchev/Cyberwarfare>
12. <http://del.icio.us/DDanchev/PSYOPS>
13. <http://del.icio.us/DDanchev/Intelligence>

447

x

## **Mobile Devices Hacking Through a Suitcase (2006-08-04 04:27)**

[1]

[2]Define:nerd



*" Luca Carettoni and Claudio Merloni are security consultants at Milan, Italy-based Secure Network. The two created the BlueBag to raise awareness about the potential of attacks against Bluetooth-enabled devices, they said in an interview at the Black Hat security event in Las Vegas. The BlueBag is a roll-aboard suitcase filled with hardware. That gear is loaded with software to scan for Bluetooth devices and launch attacks against those, the two men said. We started evaluating how Bluetooth technology was spread in a metropolitan area, Carettoni said. We went around airports,*

*offices and shopping malls and realized that a covered bag can be used quite effectively for malicious purposes. "*

Outstanding execution of the idea, I still wonder what would the content of the suitcase look like through an X-ray if

they ever get to pass through one of course. Go through the entire [3]photo session at [4]Black Hat 2006, by Joris

Evers @CNET NEWS.com's team, as well as over the basics of [5]bluetooth [6](in)security.

1.  
<http://photos1.blogger.com/blogger/1933/1779/1600/Bluebag2.1.jpg>
2. <http://www.google.com/search?hl=en&q=define%3Anerd>
3. [http://news.com.com/2300-7349\\_3-6102103-1.html](http://news.com.com/2300-7349_3-6102103-1.html)
4. <http://www.blackhat.com/html/bh-usa-06/bh-usa-06-schedule.html>
5. <http://www.securityfocus.com/infocus/1830>

6. <http://www.securityfocus.com/infocus/1836>

449

x

## **Future in Malicious Code 2006 (2006-08-05 17:43)**

[1]

What's new on the [2]malware front? Quite some [3]new developments to be included in Q2's summary

for 2006, I'm about to finalize any time now. Just came across to a [4]great continuation of my original [5]Malware

- Future Trends publication, this time courtesy of the Royal Canadian Mounted Police, [6]quoting and further

expanding the discussion on my key points :

- Mobile malware will be successfully monetized
- Localization as a concept will attract the coders' attention
- Open Source Malware
- Anonymous and illegal hosting of (copyrighted) data
- The development of Ecosystem
- Rise in encryption and packers
- 0day malware on demand
- Cryptoviral extortion / Ransomware will emerge
- When the security solutions (antivirus etc.) ends up the security problem itself

- Intellectual property worms
- Web vulnerabilities, and web worms - diversity and explicit velocity
- Hijacking botnets and infected PCs
- Interoperability will increase the diversity and reach of the malware scene

A brief summary :

*" This report will provide an overview of the numerous malicious code trends experts are observing and those they predict will be seen in the foreseeable future. This is not a document that will chart the future of malicious code as that would be impossible. Malware writers move very quickly. They are adaptable and very often they are exploiting vulnerabilities before the rest of the security industry is fully aware of them. Their flexibility and reaction speed is essential if they wish to continue to make a profit and stay ahead of the anti-virus companies who are constantly devising new ways to detect and remove hostile code. As a result, some of the trends covered in this document may never fully evolve and others that have not been mentioned will, no doubt, appear. This document will give readers a better sense of what is coming "down the pipe" and perhaps, a better idea of what to look for when dealing with tomorrow's malicious code. "*

Professionally [7]questioning a vendor's or mogul's self-mythology is the anti-mogul speciality. Don't just slice

the threat on pieces and take credit for slicing it, let's discuss the pie itself.

Meanwhile, keep an eye on my [8]Delicious Information Warfare summaries, and [9]syndicate them if time

equals [10]opportunities.

1.

[http://photos1.blogger.com/blogger/1933/1779/1600/Malicious\\_Pacman.jpg](http://photos1.blogger.com/blogger/1933/1779/1600/Malicious_Pacman.jpg)

2. <http://ddanchev.blogspot.com/2006/02/recent-malware-developments.html>

3. <http://ddanchev.blogspot.com/2006/07/malware-search-engine.html>

4. [http://www.rcmp-grc.gc.ca/tsb/pubs/it\\_sec/r2-002\\_e.pdf](http://www.rcmp-grc.gc.ca/tsb/pubs/it_sec/r2-002_e.pdf)

5.

<http://www.packetstormsecurity.org/papers/general/malware-trends.pdf>

6. <http://ddanchev.blogspot.com/2006/07/security-research-reference-coverage.html>

7. <http://ddanchev.blogspot.com/2006/06/bedtime-reading-rome-inc.html>

8. <http://ddanchev.blogspot.com/2006/07/delicious-information-warfare-2707.html>

9. <http://del.icio.us/rss/DDanchev>

10. <http://del.icio.us/DDanchev>

450

x

## **DVD of the Weekend - The Final Cut (2006-08-06 20:26)**

[1]

This [2]weekend's featured DVD is a marvelous representation of a full-scale 1984 type of mass surveillance

society, but compared to an utopian party acting as the caring BigBrother, here it's the inavitable advances of

technology, and availability of services leading to the ultimate digital preservation of our entire living - through our own eye-embedded implants. Worth taking your time to watch this "remixing" of reality leading to the ultimate saint, but I have to agree with SFAM's comments on the "usefulness" of the technology for compiling a 30 min funeral clip only. The rest is the plot itself.

A brief [3]summary of [4]The Final Cut :

*" In a near undefined future, people may have a Zoe microchip implanted in their nervous system to permit*

*their families retrieve the best moments of their memories and watch on video after their deaths. This process is*

*called "Rememory" and Alan H. Hakman (Robin Williams), a man traumatized by an incident in his childhood, is the best cutter of the Eye Tech Corporation. The company is facing groups that oppose to the "Rememory" and the ex-cutter*

*Fletcher (Jim Caviezel) is leading these opponents. When Alan is assigned to prepare the final cut of the*

*memories of the Eye Tech lawyer Charles Bannister, his Zoe chip is disputed by Fletcher. Meanwhile, Alan finds that*

*he has also an implanted microchip, which is against the rules of a cutter. "*

You can also go through [5]CyberPunkReview's comments and snapshots of The Final Cut.

### **Related resources:**

[6]Surveillance

[7]Privacy

**UPDATE:** Seems like [8]Blogspot is only searching through 7 out of my [9]209 posts, and ignoring the conspir-

acy theory you can still do it the old fashioned way -

[10]Surveillance, [11]Privacy, [12]Malware, [13]Censorship,

[14]Cyber terrorism, [15]Intelligence, etc.

1. [http://photos1.blogger.com/blogger/1933/1779/1600/th-02\\_300dpi.jpg](http://photos1.blogger.com/blogger/1933/1779/1600/th-02_300dpi.jpg)

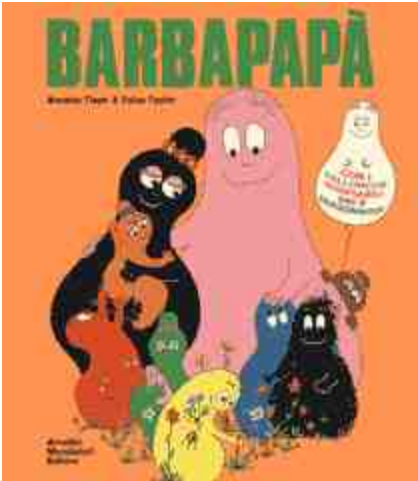
2. <http://ddanchev.blogspot.com/2006/07/dvd-of-weekend-path-to-war.html>

3. <http://www.imdb.com/title/tt0364343/plotsummary>

4. <http://www.imdb.com/title/tt0364343/>

5. <http://www.cyberpunkreview.com/movie/decade/2000-current/final-cut/>

6. <http://del.icio.us/DDanchev/Surveillance>
7. <http://del.icio.us/DDanchev/Privacy>
8. <http://search.blogger.com/?q=blogurl:ddanchev.blogspot.com&hl=en&ie=UTF-8&ui=blg>
9. <http://www.google.com/search?hl=en&lr=&q=site%3Addanchev.blogspot.com>
10. <http://www.google.com/search?hl=en&lr=&q=site%3Addanchev.blogspot.com+surveillance>
11. <http://www.google.com/search?hl=en&lr=&q=site%3Addanchev.blogspot.com+privacy>
12. <http://www.google.com/search?hl=en&lr=&q=site%3Addanchev.blogspot.com+malware>
13. <http://www.google.com/search?hl=en&lr=&q=site%3Addanchev.blogspot.com+censorship>
14. <http://www.google.com/search?hl=en&lr=&q=site%3Addanchev.blogspot.com+cyber+terrorism>
15. <http://www.google.com/search?hl=en&lr=&q=site%3Addanchev.blogspot.com+intelligence>



## **Malware Bot Families, Technology and Trends (2006-08-07 00:43)**

[1]

In case you want to know more about the evolution of bots, and ease of assem-

bling a botnet, why families take the largest zombie share compared to single bachelors only, or which technologies

dominate the threatscape - go through the slides of this study on identifying "interesting" bot technologies within a large malware collection. [2]Bot Feature & Technology Trends by Robert Lyda also highlights distribution of bot

variants from the following families :

**GaoBot**

**SpyBot**

**MyTob**

**PolyBot**



**PoeBot**

**gBot**

**BrepiBot**

**DanishBot**

**NetBot**

**KvdBot**

**TriBot**

**TongBot**

**SdBot**

**KwBot**

**BugBot**

As well as :

- Emergence of Bots as of eggdrop's 1993 appearance
- 2005 Bot Family Percentage per Month
- Bot Feature Percentage of All Variants
- Bot Feature Percentage Over All Variants
- Bot Technology Trends for 2005
- Bot Packing Analysis
- Prelevance of the Top 12 Packing Tools

To bottom line - bot families result in anti virus software detecting over 200,000 pieces of malware already,

trouble is the majority of them have long converted into family members rather than staying bachelors only as it used

to be. Malware on demand and Open Source Malware, combined with the ease of packing, are definitely making their impact.

452

### **Related resources and posts:**

[3]Malware

[4]Splitting a Botnet's Bandwidth Capacity

[5]An Intergalactic Security Statement

[6]Malware Search Engine

1.

[http://photos1.blogger.com/blogger/1933/1779/1600/Barba Papa\\_n\\_Family.gif](http://photos1.blogger.com/blogger/1933/1779/1600/Barba_Papa_n_Family.gif)

2.

[http://www.gtisc.gatech.edu/aroworkshop/ppt/BotnetTrends\\_Lyda.ppt](http://www.gtisc.gatech.edu/aroworkshop/ppt/BotnetTrends_Lyda.ppt)

3. <http://del.icio.us/DDanchev/Malware>

4. <http://ddanchev.blogspot.com/2006/07/splitting-botnets-bandwidth-capacity.html>

5. <http://ddanchev.blogspot.com/2006/07/intergalactic-security-statement.html>

6. <http://ddanchev.blogspot.com/2006/07/malware-search-engine.html>

453

x

## **JitterBugs - Covert Keyboard Communication Channels (2006-08-09 05:27)**

[1]WarTyping, [2]keyboard acoustic emanations, and here comes a full-scale covert espionage tool recently

discussed in an in-depth research at the 15th USENIX Security Symposium. Researchers at the CS department of

University of Pennsylvania developed a working prototype of a [3]JitterBug Covert Channel :

" *This paper introduces **JitterBugs**, a class of inline interception mechanisms that covertly transmit data by perturbing the timing of input events likely to affect externally observable network traffic. **JitterBugs** positioned at input devices deep within the trusted environment (e.g., hidden in cables or connectors) can leak sensitive data without*

*compromising the host or its software. In particular, we show a practical **Keyboard JitterBug** that solves the data exfiltration problem for keystroke loggers by leaking captured passwords through small variations in the precise times at which keyboard events are delivered to the host. Whenever an interactive communication application (such as*

*SSH, Telnet, instant messaging, etc) is running, a receiver monitoring the host's network traffic can recover the leaked data, even when the session or link is encrypted. Our experiments suggest that simple **Keyboard JitterBugs** can be a practical technique for capturing and exfiltrating typed secrets under conventional Oses and interactive network*

*applications, even when the receiver is many hops away on the Internet. "*

The trade-off remains on whether [4]physically restoring the device would remain undetected, compared to

directly streaming the output outside the network. I'll go for the covert network timing whereas insecurities and

flexibility are always a matter of viewpoint.

**UPDATE:** The future defined - [5]Projection Keyboards

### **Related resources:**

[6]Espionage Ghosts Busters

[7]Covert Channel

[8]Gray-World Team

[9]IP Covert Timing Channels: An Initial Exploration

[10]Information Theory of Covert Timing Channels

[11]Detection of Covert Channel Encoding in Network Packet Delays

1. <http://www.wartyping.com/>

2. <http://www.almaden.ibm.com/software/projects/hdb/Publications/papers/ssp04.pdf>
3. [https://db.usenix.org/events/sec06/tech/shah/shah\\_html/index.html](https://db.usenix.org/events/sec06/tech/shah/shah_html/index.html)
4. <http://www.keyghost.com/>
5. <http://www.alpern.org/weblog/stories/2003/01/09/projectionKeyboards.html>
6. <http://ddanchev.blogspot.com/2006/05/espionage-ghostbusters.html>
7. [http://en.wikipedia.org/wiki/Covert\\_channel](http://en.wikipedia.org/wiki/Covert_channel)
8. <http://gray-world.net/>
9. <http://www.cs.georgetown.edu/~clay/research/pubs/cabuk.cs2004.pdf>
10. [http://www.eecs.berkeley.edu/~ananth/2005+/Aaron/VA\\_ArmeniaNew.pdf](http://www.eecs.berkeley.edu/~ananth/2005+/Aaron/VA_ArmeniaNew.pdf)
11. <http://www.ists.dartmouth.edu/library/149.pdf>



## **Big Momma Knows Best (2006-08-09 06:06)**

[1]

Wish it was the [2]Chinese equivalent of Big Brother I'm refering to, in this

case it's [3]a mother of six tracking down teenagers who toilet-papered her house, and mind you, she didn't even

bother to use MySpace, instead :

*" Base persuaded supermarket managers to tally daily toilet-paper buys for the week and a Stater Bros. man-*

*ager said there was a run on bathroom tissue two days before her home was vandalized. At 7:30 p.m. Feb. 17,*

*someone bought 144 rolls of toilet paper, cheese, dog food, flour and plastic forks, the same items found on her lawn and house. It was a cash transaction, making it difficult to trace the purchaser, but the store had video surveillance.*

*The video showed four teenagers making the purchase, one of them wearing a Norco High School letterman's jacket*

*with a name stitched across the back. The store's parking lot surveillance camera showed the truck they were*

*using. Base then borrowed a Norco High yearbook and used online databases to get the name, phone numbers and addresses of the teens on the store tape. "*

One question remains though. If she managed to socially engineer the supermarket's staff to pass her transac-

tions info, even a surveillance camera footage, I wonder where they were shopping from, and would her detective

work findings hold in court given how they were obtained. What if they used a distributed shopping practice?

You may also find a previous post on [4]Big Brother in the Restroom, a relevant one.

**UPDATE:** [5]Great post at Angela Gunn's Tech \_Space. Keep your friends close, your neighbors closer!

1. [http://photos1.blogger.com/blogger/1933/1779/1600/big\\_mama.jpg](http://photos1.blogger.com/blogger/1933/1779/1600/big_mama.jpg)
2. [http://en.wikipedia.org/wiki/Big\\_mama](http://en.wikipedia.org/wiki/Big_mama)
3. [http://news.yahoo.com/s/ap/toilet\\_paper\\_caper](http://news.yahoo.com/s/ap/toilet_paper_caper)
4. <http://ddanchev.blogspot.com/2006/06/big-brother-in-restroom.html>
5. [http://blogs.usatoday.com/techspace/2006/08/big\\_brother\\_li.html](http://blogs.usatoday.com/techspace/2006/08/big_brother_li.html)

## **AOL's Search Leak User 4417749 Identified (2006-08-10 00:21)**

[1]

A Chief Privacy Officer and basic common sense anyone?

As you all know, during the weekend [2]20M search queries of 650,000 AOL users leaked, and are all over the

Internet available for download. It's simple unbelievable that the only measure to ensure the privacy of the data was

the "unique ID", and how often does the excuse of improving search results pop out. No need for subpoenas this time, but basic use of filtering techniques.

Seems like [3]AOL searcher 4417749 has been identified by a NYtimes reporter :

*" Buried in a list of 20 million Web search queries collected by AOL and recently released on the Internet is user No. 4417749. The number was assigned by the company to protect the searcher's anonymity, but it was not much*

*of a shield. No. 4417749 conducted hundreds of searches over a three-month period on topics ranging from "numb*

*fingers" to "60 single men" to "dog that urinates on everything." And search by search, click by click, the identity of AOL user No. 4417749 became easier to discern. There are queries for "landscapers in Lilburn, Ga," several people*

*with the last name Arnold and "homes sold in shadow lake subdivision gwinnett county georgia." It did not take much*



*investigating to follow that data trail to Thelma Arnold, a 62-year-old widow who lives in Lilburn, Ga., frequently*

*researches her friends' medical ailments and loves her three dogs. "Those are my searches," she said, after a reporter read part of the list to her. "*

Hope AOL gets to win the [4]Big Brother Awards, nominated for sure.

### **Related resources and posts:**

[5]Privacy

[6]Still worry about your search history and BigBrother?

[7]The Feds, Google, MSN's reaction, and how you got "bigbrothered"?

[8]What search engines know, or may find out about us?

[9]Security vs Privacy or what's left from it

[10]Snooping on Historical Click Streams

[11]Brace Yourself - AOL to Enter Security Business

1.

[http://photos1.blogger.com/blogger/1933/1779/1600/Caring\\_Big\\_Brother.0.gif](http://photos1.blogger.com/blogger/1933/1779/1600/Caring_Big_Brother.0.gif)

2. <http://www.gregsadetsky.com/aol-data/>

3.

[http://www.nytimes.com/2006/08/09/technology/09aol.html?ei=5065&en=f83b62efc45c1112&\\_amp;\\_amp;ex=1155700800&p](http://www.nytimes.com/2006/08/09/technology/09aol.html?ei=5065&en=f83b62efc45c1112&_amp;_amp;ex=1155700800&p)

[artner=MYWAY&pagewanted=print](#)

4. <http://www.privacyinternational.org/bba>
5. <http://del.icio.us/DDanchev/Privacy>
6. <http://ddanchev.blogspot.com/2006/01/still-worry-about-your-search-history.html>
7. <http://ddanchev.blogspot.com/2006/01/feds-google-msns-reaction-and-how-you.html>
8. <http://ddanchev.blogspot.com/2006/02/what-search-engines-know-or-may-find.html>
9. <http://ddanchev.blogspot.com/2006/03/security-vs-privacy-or-whats-left-from.html>
10. <http://ddanchev.blogspot.com/2006/05/snooping-on-historical-click-streams.html>
11. [http://ddanchev.blogspot.com/2006/06/brace-yourself-aol-to-enter-security\\_09.html](http://ddanchev.blogspot.com/2006/06/brace-yourself-aol-to-enter-security_09.html)

456

x

## **Analyzing the Intelligence Analysts' Factors of Productivity (2006-08-10 01:18)**

[1]

Outstanding perspective, given the author is an ex-CIA analyst himself. Controversial to the common wisdom

of a Project Manhattan type of departmental separation – everyone's working to achieve the same goal, whereas no

one knows what the others are doing – there's a growing trend of better analyzing and responding to an intelligence

analyst's productivity needs. [2]Watchin' the Analysts greatly describes the [3]Intelligence Community's efforts to

sense and respond to these growing trends of collaboration, in between figuring out how to balance the possible

security implications. Great reading, especially the infamous news headline on how the [4]CIA got "hacked" through an internal unofficial communication chat room, one that they were unaware of by the time. The paper discusses

[5]LinkedIn, [6]Del.icio.us, Blogs, and highlights the basic truth that " **Anything You Can Do, I Can Do Meta..**", an excerpt :

*" Analysts interact among themselves, as a complex community web of knowledge. Analysis of those sorts of*

*networks would be worthwhile, and is being done in the commercial sector, through a variety of tools. In the fall of 2000, the CIA shut down a so-called "chat room" operating unofficially over Agency networks; four employees lost*

*their jobs, with other employees and contractors given reprimands. I had left the Agency in 1994, but numerous of*

*those involved were friends and former colleagues. My impression was that what occurred was more embarrassing*

*than threatening, and that agency management ought to understand how and why such virtual communities form—*

*whether they're facilitated or frustrated by the "official" infrastructure—and appreciate their value. Various network*

*visualization tools would have readily revealed anomalous (at least as far as official business was concerned) traffic, but analysts will want and need an environment that fosters creativity and community, and ought to be given one. "*

However, there's [7]a certain degree of internal censorship going on, the way employers often have strict

guidelines on employees blogging activities, the CIA recently fired an analyst over an internal blog posting related to

the Geneva Convention and torture. [8]Risk management solutions, besides visualization are, of course, taking place as well.

### **Related resources and posts:**

[9]Intelligence

[10]Visualization, Intelligence and the Starlight Project

[11]"IM me" a strike order

[12]Covert Competitive Intelligence

[13]India's Espionage Leaks

[14]Japan's Reliance on U.S Spy Satellites and Early Warning Missile Systems

1.

[http://photos1.blogger.com/blogger/1933/1779/1600/Intelligence\\_Cycle.gif](http://photos1.blogger.com/blogger/1933/1779/1600/Intelligence_Cycle.gif)

2. <http://www.stapleton-gray.com/papers/ia05-full.pdf>

3. <http://www.gpoaccess.gov/int/int023.html>
4. [http://www.theregister.co.uk/2000/12/01/cia\\_sacks\\_four\\_in\\_secret/](http://www.theregister.co.uk/2000/12/01/cia_sacks_four_in_secret/)
5. <http://www.linkedin.com/>
6. <http://del.icio.us/DDanchev>
7. <http://www.washingtonpost.com/wp-dyn/content/article/2006/07/20/AR2006072001816.html>
8. <http://ddanchev.blogspot.com/2005/12/insiders-insights-trends-and-possible.html>
9. <http://del.icio.us/DDanchev/Intelligence>
10. <http://ddanchev.blogspot.com/2006/01/visualization-intelligence-and.html>
11. <http://ddanchev.blogspot.com/2006/04/im-me-strike-order.html>
12. <http://ddanchev.blogspot.com/2006/05/covert-competitive-intelligence.html>
13. <http://ddanchev.blogspot.com/2006/07/indias-espionage-leaks.html>
14. <http://ddanchev.blogspot.com/2006/07/japans-reliance-on-us-spy-satellites.html>

## Malware Statistics on Social Networking Sites (2006-08-10 02:11)

[1]

Huge traffic aggregators such as the majority of social networking sites, attract not only huge percentage

of the Internet's population on a regular basis, but also malware authors taking advantage of the medium as an

infection vector – and why not as a propagation one as well?

ScanSafe just came up with some nice stats on [2]the average number of social networking pages hosting mal-

ware - **based on five billion web requests, there's one piece of malware hosted in 600 social networking pages :**

*" According to an analysis of more than five billion Web requests in July, ScanSafe found that on average, up to one in 600 profile pages on social-networking sites hosted some form of malware. The company also reported that*

*the use of social-networking sites, often assumed to be popular only with teens, accounted for approximately 1*

*percent of all Web use in the workplace. "Social-networking sites have been newsworthy because of the concern over*

*our children's safety, but beyond unsafe contact with harmful adults, these sites are an emerging and potentially ripe threat vector that can expose children to harmful software," said Eldar Tuvey, CEO and co-founder, ScanSafe. "Users*

*are frequently subject to unwanted spyware and adware that can compromise their PCs, track online behavior and degrade PC performance. "*

SpiDynamics recent research into [3]Detecting, Analyzing, and Exploiting Intranet Applications using JavaScript

, [4]Hacking RSS and Atom Feed Implementations, and the [5]countless web application vulnerabilities in popular

portals turn this into a malware author's wet dream come true. You can also go through my [6]key points on web

application malware I made at the beginning of 2006, the "best" is yet to come.

### **Related resources and posts:**

[7]Malware

[8]Malware Targets Social Networks - podcast

[9]The Current State of Web Application Worms

[10]Web Application Email Harvesting Worm

1.

[http://photos1.blogger.com/blogger/1933/1779/1600/Worm\\_Propagation.0.1.jpg](http://photos1.blogger.com/blogger/1933/1779/1600/Worm_Propagation.0.1.jpg)

2. <http://www.scansafe.net/scansafe/news/story?id=129831>

3. <http://www.spidynamics.com/spilabs/js-port-scan/>

4.

<http://www.spidynamics.com/assets/documents/HackingFeeds.pdf>

5. [http://web3.m34s11.vlinux.de/xss\\_research.htm](http://web3.m34s11.vlinux.de/xss_research.htm)
6. <http://packetstormsecurity.org/papers/general/malware-trends.pdf>
7. <http://del.icio.us/DDanchev/Malware>
8. <http://www.eweek.com/article2/0,1759,1993753,00.asp?kc=EWRSS03129TX1K0000614>
9. <http://ddanchev.blogspot.com/2006/05/current-state-of-web-application-worms.html>
10. <http://ddanchev.blogspot.com/2006/06/web-application-email-harvesting-worm.html>

458

x

## **China's Internet Censorship Report 2006 (2006-08-11 16:59)**

[1]

Censorship is as bad, as looking directly into the sun which causes [2]blindness, and still remains the among

the few key prerequisites for successfully running a [3]modern communism type of government, namely the leader's

appearance. And while it's obvious that wearing eyeglasses is supposedly making you look smarter, I'm certain that

it's not reading on candles, but censorship that's causing the overall [4]blindness of party members on average.



Human Rights Watch [5]recently [6]reseased a [7]very comprehensive report on China's Internet censorship

philosophy, technologies, social implications and the business parties involved.

Meanwhile, the blocked since 2002 [8]Blogger.com seems to be again accessible in China. A battle victory for

free speech? Don't be naive, the reason it's still accessible is that they figured out how to censor what needs to be

censored - reverse model consisting of allowing everything, and blocking as well as monitoring access to potentially

dangerous blogs. Less negative public opinion for sure, a good indication on why [9]the Great Firewall has the

potential to get breached into from within. Here are key summaries of what made me an impression:

**01.** [10]URL de-listing on Google.cn, Yahoo! China, MSN Chinese and Baidu

**02.**

[11]Comparative keyword searches on Google.cn, Yahoo!

China, MSN China, Baidu, Yahoo.com, MSN

search and Google.com

**03.**

[12]The words you never see in Chinese cyberspace - courtesy of Chinese hackers located a document

within the installation package of QQ instant messaging software :

falun, sex, tianwang, cdjp, av, bignews, boxun, chinaliberal, chinamz, chinesenewsnet, cnd, creaders, dafa, da-

jiyuan, dfdz, dpp, falu, falun, falundafa, flg, freechina, freedom, freenet, GCD, gcd , hongzhi , hrichina , huanet ,

hypermart , incest , jiangdongriji , lihongzhi ,making , minghui , minghuinews , nacb , naive , nmis , paper , peacehall , playboy , renminbao , renmingbao , rfa , safeweb, sex , simple , svdc , taip , tibetalk , triangle , triangleboy , UltraSurf

, unixbox , ustibet , voa, voachinese, wangce, wstaiji, xinsheng, yuming, zhengjian, zhengjianwang, zhenshanren,

zhuanfalun

**04.** [13]The Great Firewall of China: Keywords used to filter web content :

### **Names of People**

Bao Tong, Chen Yonglin, Cui Yingjie, Ding Jiaban, Du Zhaoyong, Gao Jingyun, Gao Zhisheng, He Jiadong, He Weifang,

Hu Xingdou, Hu Yuehua, Hua Guofeng, Huang Jingao, Jiang Mianheng, Jiang Yanyong, Jiang Zemin, Jiao Guobiao, Jin

Zhong, Li Zhiying, Liang Yuncai, Liu Jianfeng, Liu Junning, Liu Xiabobo, Nie Shubin, Nie Shubin (repeated),Sun Dawu,

Wang Binyu, Wang Lixiong, Xu Zhiyong, Yang Bin, Yang Dongping, Yu Jie, Zhang Weiyong, Zhang Xingshui, Zhang

Zuhua,Zhao Yan, Zhou Qing, Zhu Chenghu, Zhu Wenhui, Zi Yang (in English), Ziyang (in Chinese), Ziyang (in English), zzy (in English, abbreviation for Zhao Ziyang)

## **Chinese Politics**

17th party congress, Babaoshan,Beat [overthrow] the Central Propaganda Department, Blast the Central Propaganda

Department, Block the road and demand back pay, Chief of the Finance Bureau, Children of high officials, China

liberal (in English), Chinese Communist high officials, Denounce the Central Propaganda Department, Down with

the Central Propaganda Department, Impeach, Lin Zhao Memorial Award, Patriots Alliance, Patriots Alliance

(abbreviated), Patriots Alliance Web, Police chase after and kill police, Pollution lawsuit, Procedures for dismissing an official, Red Terror, Set fires to force people to relocate, Sons of high officials, The Central Propaganda Department

is the AIDS of Chinese society, Villagers fight with weapons, Wang Anshi's reform and the fall of the Northern Song

459

dynasty, Specific Issues and Events, Buy corpses, Cadres transferred from the military, Cashfiesta (English), Cat abuse, Changxin Coal Mountain, China Youth Daily staff evaluation system, Chinese orphanage, Chinese Yangshen

Yizhi Gong, Demobilized soldiers transferred to other industries, Dongyang, Dongzhou, Fetus soup, Foot and

mouth

disease, Fuzhou pig case, Gaoxin Hospital, High-speed train petition, Hire a killer to murder one's wife, Honghai Bay,

Horseracing, Jinxin Pharmaceutical, Kelemayi, Linyi family planning, Market access system, Mascot, Military wages,

No Friendlies, Prosecutor committed suicide, Pubu Ravine, Shanwei government, Suicide of deputy mayor, Suicide

of Kuerle mayor, Swiss University of Finance, Taishi village, Top ten worst cities, Wanzhou, Weitan [Village], Zhang

Chunxian welcomes supervision against corruption, Falun Gong

**Terms related to the banned Falun Gong spiritual movement, including phrases from its "Nine Commentaries"**

**manifesto against the Communist Party**

Chinese Communist Party brutally kills people, dajiyuan (in English), Defy the heavens, earth and nature. Mao

Zedong, Epoch Times, Epoch Times (written with a different character), Epoch Times news Web site, Evaluate the

Chinese Communist Party, Evaluate the Chinese Communist Party (abbreviated), falundafa (in English), flg (in English),

Fozhan Qianshou Fa, Guantong Liangji Fa, In the Chinese Communist Party, common standards of humanity don't

exist, Li Hongzhi, lihongzhi (in English), Master Li, minghui (in English), Mother and daughter accused each other,

and students and teachers became enemies, New Tang  
dynasty TV Station, Nine Commentaries, No. 1 evil cult in  
the

world, Obedient citizens under its brutal rule, People  
become brutal in violence, Chinese Communist Party, People

developed a concept of the Chinese Communist Party, but,  
People who could escape have escaped, and had people

to seek refuge with, Quit the party, Run the opposite  
direction of the so-called ideals of Communism, Shenzhou

Jiachifa, Spring Festival Gala of the World's Chinese, Steal  
people's painstaking work, Truth, Compassion, Tolerance

[Falungong slogan], Zhenshanren (in English) [same slogan  
in English]

### **Overseas Web Sites, Publications and Dissident Groups**

Century China Foundation, China Issues Forum, China  
Renaissance Forum, China Society Forum, China Spring,

Chinese Current Affairs, Chinese World Forum,  
EastSouthWestNorth Forum, EastWestSouthNorth Forum,  
Forum of

Wind, Rain and the Divine Land, Freedom and Democracy  
Forum, Freedom to Write Award, Great China Forum, Han

Style, Huatong Current Affairs Forum, Huaxia Digest, Huayue  
Current Affairs Forum, Independent Chinese PEN Center,

Jimaixin Collection, Justice Party Forum, New Birth Web, New  
Observer Forum, North American Freedom Forum,

reminbao (in English), remingbao (in English), Small Reference, Spring and Summer Forum, Voice of the People

Forum, Worldwide Reader Forum, You Say I Say Forum, Zhengming Forum, Zhidian Jiangshan Forum, Zhongshan

Wind and Rain Forum

## **Taiwan**

Establish Taiwan Country Movement Organization, Great President Chen Shui-bian, Independent League of Taiwan

Youth, Independent Taiwan Association, New Party, Taiwan Freedom League, Taiwan Political Discussion Zone

## **Ethnic Minorities**

East Turkestan, East Turkestan (abbreviated), Han-Hui conflicts [ethnic conflicts], Henan Zhongmu, Hui [muslim ethnic

minority] rebellion, Hui village, Langcheng Gang, Nancheng Gang, Nanren Village, Tibet independence, Xinjiang

independence, Zhongmu County

## **Tiananmen Square**

Memoirs of June 4 participants, Redress June 4, Tiananmen videotape, Tiananmen incident, Tiananmen massacre,

Tiananmen generation, World Economic Herald

## **Censorship**

Cleaning and rectifying Web sites, China's true content, Internet commentator, News blockade

## **International**

460

Indonesia, North Korea falls out with China, Paris riots, Tsunami

## **Other**

Armageddon, Bomb, Bug, Handmade pistol, Nuclear bomb, Wiretap, Chinese People Tell the Truth, Chinese People

Justice and Evil, China Social Progressive Party, Chinese Truth Report, Dazhong Zhenren Zhenshi, Jingdongriji (English), Night talk of the Forbidden City, People's Inside Information and Truth

Take your time to understand the [14]Twisted Reality courtesy of [15]China's Internet Censorship efforts, and

learn more on [16]how to undermine censorship.

## **Related resources and recent posts:**

[17]Censorship

[18]China's Interest of Censoring Mobile Communications

[19]South Korea's View on China's Media Control and Censorship

1.

<http://photos1.blogger.com/blogger/1933/1779/1600/Censorship.0.jpg>

2.

<http://photos1.blogger.com/blogger/1933/1779/1600/Censorship.gif>

3. [http://en.wikipedia.org/wiki/Communist\\_Party\\_of\\_China](http://en.wikipedia.org/wiki/Communist_Party_of_China)
4. <http://www.hinduonnet.com/fline/fl2207/images/20050408000905401.jpg>
5. <http://hrw.org/chinese/docs/2006/08/09/china13961.htm>
6. <http://www.hrw.org/reports/2006/china0806/>
7. <http://www.hrw.org/reports/2006/china0806/china0806webwcover.pdf>
8. [http://www.cio.com/blog\\_view.html?CID=23811](http://www.cio.com/blog_view.html?CID=23811)
9. <http://www.forbes.com/business/global/2006/0227/018A.html>
10. <http://www.hrw.org/reports/2006/china0806/Table1Appendix.pdf>
11. <http://www.hrw.org/reports/2006/china0806/Table2Appendix.pdf>
12. [http://www.hrw.org/reports/2006/china0806/9.htm#\\_Toc142395838](http://www.hrw.org/reports/2006/china0806/9.htm#_Toc142395838)
13. [http://www.hrw.org/reports/2006/china0806/10.htm#\\_Toc142395839](http://www.hrw.org/reports/2006/china0806/10.htm#_Toc142395839)



14. <http://ddanchev.blogspot.com/2006/01/twisted-reality.html>
15. <http://ddanchev.blogspot.com/2006/02/chinese-internet-censorship-efforts.html>
16. <http://irrepressible.info/>
17. <http://del.icio.us/DDanchev/Censorship>
18. <http://ddanchev.blogspot.com/2006/07/chinas-interest-of-censoring-mobile.html>
19. <http://ddanchev.blogspot.com/2006/07/south-koreas-view-on-chinas-media.html>

461



### **Anti Satellite Weapons (2006-08-12 03:01)**

[1]

Continuing the discussion on the ongoing weaponization of space, and the

consequently emerging space warfare arms race. Micro satellites directly matching other satellites trajectories, and

taking advantage of high energy concentration in the form of lasers? For sure, but why bother [2]damaging an entire

reconnaissance satellite when you can basically spray its lenses to prevent it from using its core function:

*" But the ability to operate autonomously near another satellite could also be used for offensive purposes, says Theresa Hitchens of the Center for Defense Information in Washington DC, US. If an ANGELS-like satellite were sent*

*towards another country's satellite, it could be used as a weapon, she says. "It's not far fetched to think that you could equip such little satellites with radio frequency jammers or technologies to block image capability," she told New Scientist. For example, a mini satellite could spray paint on the lens of a satellite's camera in order to blind it, she says. "There's a huge potential for this to be used as an anti-satellite weapon of some sort. "*

Quite a creative space provocation, isn't it?

### **Related resources and posts:**

[3]Anti Satellite Weapons

[4]Anti Satellite Weapons @ FAS

[5]Is a Space Warfare arms race really coming?

[6]Weaponizing Space and the Emerging Space Warfare Arms Race

1.

<http://photos1.blogger.com/blogger/1933/1779/1600/xss11.jpg>

2. <http://www.newscientistspace.com/article.ns?id=dn9674&print=true>
3. [http://en.wikipedia.org/wiki/Anti-satellite\\_weapon](http://en.wikipedia.org/wiki/Anti-satellite_weapon)
4. <http://www.fas.org/spp/military/program/asat/index.html>
5. <http://ddanchev.blogspot.com/2006/03/is-space-warfare-arms-race-really.html>
6. <http://ddanchev.blogspot.com/2006/07/weaponizing-space-and-emerging-space.html>

462

x

## **Bed Time Reading - Symbian OS Platform Security: Software Development Using the Symbian OS Security**

**Architecture (2006-08-12 03:21)**

[1]

Prr, did I hear someone start counting mobile malware samples, prr?

Try getting to know the OS itself, the main proof of concept faciliator representing today's constantly growing

mobile [2]malware family. A review of this [3]recommended bed time reading book :

*" Symbian OS is an advanced, customizable operating system, which is licensed by the world's leading mobile*

*phone manufacturers. The latest versions incorporate an enhanced security architecture designed to protect the interests of consumers, network operators and software developers. The new security architecture of Symbian OS v9 is relevant to all security practitioners and will influence the decisions made by every developer that uses Symbian OS in the creation of devices or add-on applications. Symbian OS Platform Security covers the essential concepts and presents the security features with accompanying code examples. This introductory book highlights and explains:*

- \* the benefits of platform security on mobile devices*
- \* key concepts that underlie the architecture, such as the core principles of 'trust', 'capability' and data 'caging'*
- \* how to develop on a secure platform using real-world examples*
- \* an effective approach to writing secure applications, servers and plug-ins, using real-world examples*
- \* how to receive the full benefit of sharing data safely between applications*
- \* the importance of application certification and signing from the industry 'gatekeepers' of platform security*
- \* a market-oriented discussion of possible future developments in the field of mobile device security"*

Malware authors indeed have [4]financial incentives to futher continue recompiling publicly available PoC mo-

mobile malware source code, and it's the purchasing/identification features phones, opening a car with an SMS, opening

a door with an SMS, purchasing over an SMS or direct barcode scanning, mobile impersonation scams, harvesting

phone numbers of infected victims, as well as unknowingly interacting with premium numbers are the things about

to get directly abused – efficiently and automatically. And whereas there are more people on Earth with mobile

phones compared to those with PCs, it doesn't necessarily mean everyone's having a smart phone – perhaps Bill

Gates "remarkable" [5] cash on the poor proposition could soon undermine the [6] \$100 laptop one.

People are getting more aware on the social engineering basics of today's mobile malware, and running a mo-

mobile phone anti-virus would be nothing more than a marketer's dream come true – end users positioning themselves

as security savvy buyers. Mobile operators tend to have God's eye view on their networks, therefore epidemics are

far from reality, targeted attacks (events and places where the masses gather or pass by), and directly exploiting the

lack of awareness in certain regions could make an impact. South Korea's advances in mobile communications let its

citizens have more phone bandwidth than an average ADSL user, but I would still have to see this getting abused at a

level going beyond the sophisticated impersonation scams going on all the time.

Worth taking your time to read this book, go through Chapter 1 discussing "[7]Why a Secure Platform?" is the basics of mobile devices security, as well.

### **Related posts:**

[8]Privacy issues related to mobile and wireless Internet access

[9]Digital forensics - efficient data acquisition devices

[10]The Cell-phone Industry and Privacy Advocates VS Cell Phone Tracking

[11]Mobile Devices Hacking Through a Suitcase

[12]Bed Time Reading - The Baby Business

463

[13]Bed Time Reading - Rome Inc.

1.  
[http://photos1.blogger.com/blogger/1933/1779/1600/Symbian\\_OS\\_Security.0.jpg](http://photos1.blogger.com/blogger/1933/1779/1600/Symbian_OS_Security.0.jpg)

2. <http://ddanchev.blogspot.com/2006/08/malware-bot-families-technology-and.html>

3. <http://eu.wiley.com/WileyCDA/WileyTitle/productCd-0470018828.html>

4.  
<http://www.symantec.com/avcenter/venc/data/trojan.redbro>

[wser.a.html](#)

5. <http://www.engadget.com/2006/01/30/gates-proposes-cellphones-as-alternative-to-olpc/>

6. <http://laptop.media.mit.edu/>

7. <http://eu.wiley.com/WileyCDA/WileyTitle/productCd-0470018828.html>

8. <http://ddanchev.blogspot.com/2006/03/privacy-issues-related-to-mobile-and.html>

9. <http://ddanchev.blogspot.com/2006/04/digital-forensics-efficient-data.html>

10. <http://ddanchev.blogspot.com/2006/05/cell-phone-industry-and-privacy.html>

11. <http://ddanchev.blogspot.com/2006/08/mobile-devices-hacking-through.html>

12. <http://ddanchev.blogspot.com/2006/05/bedtime-reading-baby-business.html>

13. <http://ddanchev.blogspot.com/2006/06/bedtime-reading-rome-inc.html>



Copyright © 2000 United Feature Syndicate, Inc.

## AOL's Search Queries Data Mined (2006-08-16 06:38)

[1]

While one of [2]AOL's searchers was publicly identified, enthusiasts are [3]tweaking, and [4]randomly scrolling the

then leaked, now publicly available search queries data. Here's someone that's neatly data mining and providing

relevant summary of the top result sites, and the top keywords. [5]SEO Sleuth :

*" was created out of the recently released AOL search data. Welcome to the AOL Keyword Analyser. This tool*

*provides insights that have never before been publically available on the web. I claim: First tool on the web as far as I know that allows you to view what keywords people searched for it in search engines. First time you can see*

*how much organic traffic each site gets from a search engine. First opportunity the public can see how many clicks*

*individual SERPs get. "*

Surprising results speaking for the quality of the audience by themselves. Meanwhile, the [6]EFF is naturally



taking actions.

### **Related posts:**

[7]Data mining, terrorism and security

[8]Shots From the Wild - Terrorism Information Awareness Program Demo Portal

1. <http://photos1.blogger.com/blogger/1933/1779/1600/DataMiningResults.2.gif>
2. <http://ddanchev.blogspot.com/2006/08/aols-search-leak-user-4417749.html>
3. <http://www.aolsearchdatabase.com/>
4. <http://projects.cocaman.net/aol500k/aol500k.swf>
5. <http://www.seosleuth.com/site/>
6. <http://action.eff.org/aolsearch>
7. <http://ddanchev.blogspot.com/2006/03/data-mining-terrorism-and-security.html>
8. <http://ddanchev.blogspot.com/2006/06/shots-from-wild-terrorism-information.html>

465



**On the Insecurities of Sun Tanning (2006-08-19 20:49)**

[1]

You definitely don't need a CISSP certificate to blog on this one, just make sure you don't forget that there

should be a limit on everything, even the hugs on [2]the beach.

1.

<http://photos1.blogger.com/blogger/1933/1779/1600/beach.jpg>

2. <http://www.howstuffworks.com/sunscreen.htm>

466



## **North Korea's Strategic Developments and Financial Operations (2006-08-20 00:15)**

[1]

Catching up with the latest developments at the hottest – at least

from a national security point of view – zone in Asia. North Korea seems to be taking [2]external provocations

rather seriously, and feeling endangered for the collapse of its regime is actively working on its nuclear test sites

development, disinformation in between for sure. According to a recent article at Reuters, [3]North Korea may be

preparing nuclear bomb test :

*" ABC reported the activity at the suspected test site included the unloading of large reels of cable outside an underground facility called Pungyee-yok in northeast North Korea. It said cables can be used in nuclear testing to*

*connect an underground test site to outside observation equipment. The intelligence was brought to the attention*

*of the White House last week, the report said. Fears about North Korea's nuclear ambitions were exacerbated when*

*Pyongyang defied international warnings and fired seven missiles into waters east of the Korean peninsula on July 5. "*

Excluding an opinionated **W**eapons of **M**ass **D**eception expert's interest in developments like these, speculations remain a powerful driving force for everyone involved. Consider a basic principle in life, it is often assumed

that gathering together a bunch of handicapped people is the best solution for their "fragile" situation, compared to actually trying to integrate instead of isolate them. I find the same issue as the cornerstone when dealing

with countries on purposely isolating themselves, thus limiting the international accountability and ensuring the

continuity of the twisted reality.

Meanwhile, the U.S is actively working on closing down North Korean bank accounts, and worsening its rela-

tions with major financial institutions worldwide, in response to which North Korea is diversifying and [4]opening

accounts at 23 banks in 10 countries :

*" North Korea has opened accounts at 23 banks in 10 countries following the U.S. imposition of financial sanc-*

*tions on a bank in Macau last year, a Japanese newspaper reported Saturday. The Sankei Shimbun said on its Web*

*site the 10 countries include Vietnam, Mongolia and Russia, quoting sources familiar with North Korean affairs.*

*In September, the United States banned all American financial institutions from transacting with a Macau-based*

*bank, Banco Delta Asia, accusing it of aiding North Korea in circulation of counterfeit U.S. dollars allegedly printed in the communist state. The U.S. also confirmed last month that the Bank of China, a major Chinese lender, had*

467

*frozen all of its North Korean accounts suspected of being connected with the North's alleged counterfeiting activities.*  
"

And while China is realizing its growing economic potential, thus [5]complying with such efforts as well, **help-**

**ing the enemies of your enemies** still remain a fashionable concept in the [6]silent war.

### **Related resources and posts:**

[7]Satellite Imagery of Pre-Launch and Post-Launch at the Taepodong Launch Facility and Affected Vegetation

[8]A-Bomb North Korean Propaganda

[9]North Korea - Turn On the Lights, Please

[10]Japan's Reliance on U.S Spy Satellites and Early Warning Missile Systems

[11]Open Source North Korean IMINT Reloaded

[12]North Korea's Cyber Warfare Unit 121

1.

[http://photos1.blogger.com/blogger/1933/1779/1600/catchy\\_north\\_korean\\_propaganda.jpg](http://photos1.blogger.com/blogger/1933/1779/1600/catchy_north_korean_propaganda.jpg)

2. <http://www.kcna.co.jp/item/2004/200407/news07/26.htm>

3.

[http://today.reuters.com/news/articlenews.aspx?type=topNews&storyID=2006-08-17T215903Z\\_01\\_N17323351\\_RTRUK](http://today.reuters.com/news/articlenews.aspx?type=topNews&storyID=2006-08-17T215903Z_01_N17323351_RTRUK)

[OC\\_0\\_US-NUCLEAR-KOREA-NORTH.xml](http://OC_0_US-NUCLEAR-KOREA-NORTH.xml)

4.

[http://english.hani.co.kr/arti/english\\_edition/e\\_international/150335.html](http://english.hani.co.kr/arti/english_edition/e_international/150335.html)

5. <http://www.wsws.org/articles/2006/aug2006/korea-a19.shtml>
6. <http://en.wikipedia.org/wiki/Espionage>
7. [http://web.stratfor.com/images/asia/art/N\\_Korea-Sat.JPG](http://web.stratfor.com/images/asia/art/N_Korea-Sat.JPG)
8. <http://www.danegerus.com/weblog/images/NorK5.jpg>
9. <http://ddanchev.blogspot.com/2006/06/north-korea-turn-on-lights-please.html>
10. <http://ddanchev.blogspot.com/2006/07/japans-reliance-on-us-spy-satellites.html>
11. <http://ddanchev.blogspot.com/2006/07/open-source-north-korean-imint.html>
12. <http://ddanchev.blogspot.com/2006/07/north-koreas-cyber-warfare-unit-121.html>

468

x

## **U.S Air Force on MySpace (2006-08-22 19:14)**

[1]

Seems like the [2]U.S Air Force is joining MySpace:

*" The Air Force profile will show users five video clips that the Recruiting Service says gives them "a behind-the-scenes look at the extraordinary things airmen accomplish every day," according to a press release. Users will be*

*able to view longer videos of airmen as they fly jets, call in air strikes, navigate satellites and jump out of airplanes, the*

*service said. They also can vote on which commercial will kick off the Air Force's new "Do Something Amazing"*

*advertising campaign, scheduled for Sept. 18 during the FOX network's "Prison Break" television show. "*

It's like using a Yahoo Group mailing list to break the ice and keep it teen-friendly. Now, teens all over the U.S

know which buddy to avoid. I'm sure [3]Privacy advocates will pick this up shortly, given "someone" isn't already

[4]data mining MySpace profiles for [5]targeted propositions – of course they are.

1.  
<http://photos1.blogger.com/blogger/1933/1779/1600/flyer.1.jpg>

2. <http://www.airforcetimes.com/story.php?f=1-292925-2049378.php>

3. <http://www.commondreams.org/headlines05/0624-03.htm>

4. <http://lists.grok.org.uk/pipermail/full-disclosure/2006-June/047579.html>

5. <http://www.commondreams.org/headlines06/0117-12.htm>

469

x

**Virus Outbreak Response Time (2006-08-22 19:41)**

[1]

In a previous posts I discussed various [2]trends related to [3]malware families, and mentioned CipherTrust's

[4]Real Time PC Zombie Statistics. You might also be interested in IronPort's [5]Virus Outbreak Response Times for the last 24 hours which currently tracks, IronPort themselves, Sophos, Trend Micro, Symantec, and McAfee. Although

vendor's bias often exist, let's just say that self-serving statements can easily be verified by doing a little research on your own – it doesn't cost a fortune to run a geographically diverse honeyfarm. However, what bothers me is the vendors' constant claims on exchanging malware samples for the sake of keeping the E in front of E-Commerce, whereas

response time "achievements" often get converted into marketing benchmarks to be achieved. [6]Protecting against known malware is far more complex than it seems, and it is often arguable whether zero day malware, or known

malware has the highest impact when infecting both, corporate, and home PCs. Basically you have [7]powerful end

users getting themselves infected with months old malware and later on collectively becoming capable of causing

damage on a network that's already aiming at achieving the proactive protection level. Irony isn't it? If detailed

statistics truly matter, [8]VirusTotal has the potential to dominate the analysts community without bias.



Response times used to matter once, now it's all up to [9]proactive protection [10]approaches, and, of course,

revenue generation from both sides. Moreover, sometimes even a [11]signature based approach doesn't work,

especially when it comes to [12]packet based or web application based malware. Avoid the signatures hype and start

rethinking the concept of malware on demand, open source malware, and the growing trend of malicious software

to disable an anti virus scanner, or its ability to actually obtain the latest signatures available.

At the bottom line, [13]achieving ROSI when it comes to [14]false malware positives is yet another growing

concern for the majority of enterprises wisely spending their security dollars.

1. [http://photos1.blogger.com/blogger/1933/1779/1600/flu\\_virus.png](http://photos1.blogger.com/blogger/1933/1779/1600/flu_virus.png)
2. <http://ddanchev.blogspot.com/2006/08/future-in-malicious-code-2006.html>
3. <http://ddanchev.blogspot.com/2006/08/malware-bot-families-technology-and.html>
4. <http://ddanchev.blogspot.com/2006/06/real-time-pc-zombie-statistics.html>
5. <http://www.ironport.com/toc/>

6. <http://ddanchev.blogspot.com/2006/07/anti-virus-signatures-update-it-could.html>
7. <http://ddanchev.blogspot.com/2006/07/splitting-botnets-bandwidth-capacity.html>
8. <http://www.virustotal.com/>
9. <http://http://www.viruslist.com/en/analysis?pubid=189801874>
10. [http://www.viruslist.com/en/downloads/vlpdfs/wp\\_nikishin\\_preactive\\_en.pdf](http://www.viruslist.com/en/downloads/vlpdfs/wp_nikishin_preactive_en.pdf)
11. <http://ddanchev.blogspot.com/2006/01/why-relying-on-virus-signatures-simply.html>
12. <http://ddanchev.blogspot.com/2006/08/malware-statistics-on-social.html>
13. <http://ddanchev.blogspot.com/2006/05/valuing-security-and-prioritizing-your.html>
14. [http://www.av-test.org/down/papers/2005-11\\_vb\\_falsepos2.pdf](http://www.av-test.org/down/papers/2005-11_vb_falsepos2.pdf)

470

x

x

**Cyber Terrorism Communications and Propaganda  
(2006-08-22 20:39)**

[1]

Further expanding the previous discussion on [2]Tracking Down Internet Terrorist Propaganda, and patterns

of [3]Arabic Extremist Group Forum Messages' Characteristics, there've also been some recent developments on

[4]Hezbollah's never-ending use of U.S hosting companies as a

**media/communication/** fund raising/  
**recruitment/propaganda** platform:

*" Hezbollah used the Broadwing Communications fiber-optic network to deliver its Al-Manar web site to the*

*world last week after [5] finding a weakness in a Broadwing customer's connection. When that happened, Hezbollah television's web site was suddenly hosted, of all places, in Texas. When Broadwing discovered what had happened,*

*they cut the T1 connection to their customer until the customer resolved the problems on its end, and the Al-Manar*

*site disappeared back into the ether—only to pop up a few hours later on a server in India. Hezbollah's tactics are laid out in a brief [6] Time article that also discusses the people trying to shut Hezbollah down. And it's not the people you might think. Those in the war and security business are no doubt involved, but some of the work is done by amateurs, as well. Volunteers from the Society for Internet Research track jihadi websites and tactics across the Internet, then alert domain registrars and web hosting companies to the presence of potentially illegal material on their servers. "*

Al Manar TV has long been known for delivering Hezbollah's PSYOPS through constantly relocating its stream,

but [7]information warfare capable enemies seem to be able to hijack the signal as it recently happened. Moreover,

according to Haganah's most recent [8]Table of American Internet Service Providers of Hezbollah - [9]detailed

analyses - Register.com remains a popular choice.

Cyber terrorism is a complex and often misunderstood term that originally emerged as the direct effect of

[10]Techno Imperialism sentiments, and, of course, the balancing power of the Internet when it comes to [11]cyber

warfare capabilities. In another great research [12]Cyber Terrorism: A Study of the Extent of Coverage in Computer

Security Textbooks, the author summarized the most commonly encountered Cyber Terrorism categories and

keywords, and discussed the different explanations of the term. As for Cyber terrorism, the first issue that comes to

the mind of the average expert are the [13]SCADA systems whose IP based connectivity remains a growing concern

for governments utilizing these. [14]

Which is exactly the least issue to worry about, today's Cyber terrorism

is still maturing, tomorrow's Cyber terrorism will be taking advantage of cyber warfare capabilities on demand or

through direct recruitment/blackmailing practices of individuals capable of delivering them. [15]Here's a neat table

representing the maturity/evolution of Cyber terrorism .

For the time being, propaganda and recruitment are so far the most indirect and popular practices, whereas

the concept itself is truly maturing thus becoming even more evident. Thankfully, various researchers are already

actively combining [16]AI and various web crawling approaches while analyzing the presence of terrorists on the web

- and here's a [17]good starting point.

### **Related resources and posts:**

[18]Cyber Terrorism

[19]Hacktivism

[20]Information Warfare

[21]Cyberterrorism - don't stereotype and it's there!

[22]Cyberterrorism - recent developments

[23]The Current, Emerging, and Future State of Hacktivism

[24]Terrorist Social Network Analysis

[25]Hacktivism Tensions - Israel vs Palestine Cyberwars

1.

<http://photos1.blogger.com/blogger/1933/1779/1600/propa>

[ganda.jpg](#)

2. <http://ddanchev.blogspot.com/2006/06/tracking-down-internet-terrorist.html>

471

3. <http://ddanchev.blogspot.com/2006/05/arabic-extremist-group-forum-messages.html>

4. <http://arstechnica.com/news.ars/post/20060809-7455.html>

5. <http://www.statesman.com/business/content/business/stories/technology/08/3broadwing.html>

6. <http://www.time.com/time/world/printout/0,8816,1224273,00.html>

7. <http://www.theage.com.au/news/technology/israel-hacks-into-hezbollah-tv-radio/2006/08/02/1154198175078.html>

8. <http://haganah.org.il/harchives/005691.html>

9. <http://haganah.org.il/harchives/005690.html>

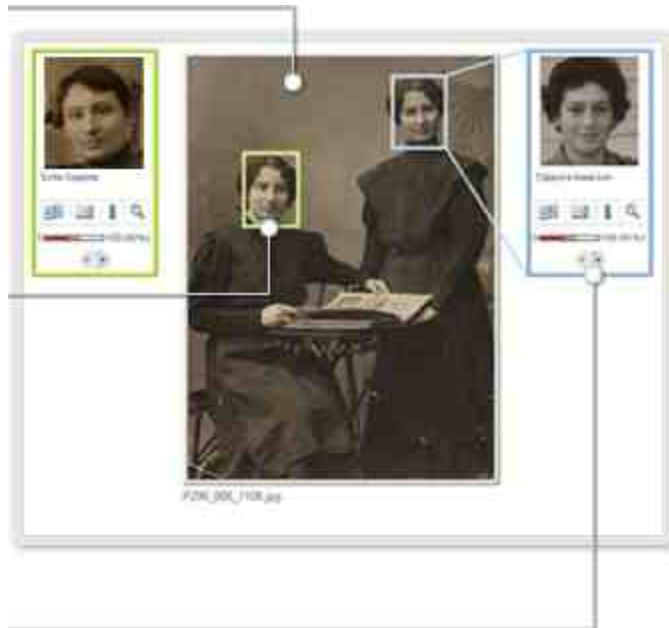
10. <http://ddanchev.blogspot.com/2006/05/techno-imperialism-and-effect-of.html>

11. <http://ddanchev.blogspot.com/2006/05/whos-who-in-cyber-warfare.html>

12. <http://www.jite.org/documents/Vol3/v3p279-289-150.pdf>
13. <http://del.icio.us/DDanchev/SCADA>
14. <http://photos1.blogger.com/blogger/1933/1779/1600/Cyberterrorism.jpg>
15. [http://www.oii.ox.ac.uk/microsites/cybersafety/extensions/pdfs/papers/maura\\_conway.pdf](http://www.oii.ox.ac.uk/microsites/cybersafety/extensions/pdfs/papers/maura_conway.pdf)
16. [http://ai.arizona.edu/research/terror/publications/ISI\\_AILab\\_submission\\_final.pdf](http://ai.arizona.edu/research/terror/publications/ISI_AILab_submission_final.pdf)
17. [http://tajdeed-list.net/pipermail/pir\\_tajdeed-list.net/2006-June/000092.html](http://tajdeed-list.net/pipermail/pir_tajdeed-list.net/2006-June/000092.html)
18. <http://del.icio.us/DDanchev/Cyberterrorism>
19. <http://del.icio.us/DDanchev/Hacktivism>
20. <http://del.icio.us/DDanchev/InformationWarfare>
21. <http://ddanchev.blogspot.com/2005/12/cyberterrorism-dont-stereotype-and-its.html>
22. <http://ddanchev.blogspot.com/2006/01/cyberterrorism-recent-developments.html>
23. <http://ddanchev.blogspot.com/2006/05/current-emerging-and-future-state-of.html>
24. <http://ddanchev.blogspot.com/2006/05/terrorist-social-network-analysis.html>

25. <http://ddanchev.blogspot.com/2006/07/hacktivism-tensions-israel-vs.html>

472



## Face Recognition At Home (2006-08-26 00:48)

[1]

In a previous post, [2]Biased Privacy Violation I mentioned two web sites, [3]DontDateHimGirl.com, [4]DontDate-

HerMan.com and the associated privacy implications out of these. Just came across to [5]MyHeritage.com whose

[6]face recognition feature works remarkably well – for relatives and everyone in between varying on the sample.

" Recognizing faces is done by algorithms that compare the faces in your photo, with all faces previously known to MyHeritage Face Recognition, through photos and meta-data contributed by yourself and other users. So the more



*photos added to the system, the more powerful it becomes. If people in your photos are not recognized well, it is*

*likely that MyHeritage.com has never encountered them before. By adding these photos to MyHeritage.com and*

*annotating the people in the photo manually, MyHeritage.com will "learn" these faces and will be able to recognize them in future photos, even in different ages of the same person's life. Note: the algorithms used by MyHeritage Face Recognition are likely to find relatives of people in your photo, due to the genetic-based facial similarities that exist between relatives. You can use this to form connections between people whom you never even knew were related. "*

Face recognition @home just got a boost and so did the obvious privacy implications out of the ever-growing

families database, and its natural abuse by interested (third) parties.

1.

[http://photos1.blogger.com/blogger/1933/1779/1600/face\\_recognition.gif](http://photos1.blogger.com/blogger/1933/1779/1600/face_recognition.gif)

2. [http://ddanchev.blogspot.com/2006/05/biased-privacy-violation\\_03.html](http://ddanchev.blogspot.com/2006/05/biased-privacy-violation_03.html)

3. <http://www.dontdatehimgirl.com/>

4. <http://dontdateherman.com/>

5. <http://www.myheritage.com/>

6. <http://www.myheritage.com/FP/Company/face-recognition.php>

## **Futuristic Warfare Technologies (2006-08-26 01:27)**

[1]

The future of warfare will definitely have to do with technologies and convergence, at least the near one.

Some logical developments such as, remote sensing intercontinental UAVs, autonomous warfare, remotely controlled

forces, network centric warfare, higher reliance on AI probability and decision-making scenarios, are just warming up

the major innovations we're about to witness – whether defensive or offensive is an entirely different topic. In the

very long term though, [2]Nano warfare, Robot wars and Cyber wars reaching the levels of VR warfare, are among

the fully realistic scenarios. Very informative slides on the [3]Future Strategic Issues/Future Warfare [Circa 2025],

and here are some important key points that made me an impression :

### **Technological Ages of Humankind**

- Hunter/Killer groups [ Million BC 10K BC]
- Agriculture [ 10K BC 1800 AD]
- Industrial [1800-1950]

- IT [1950-2020]
- Bio/NANO [2020?]
- Virtual

## **The developments**

- Chem/bio Antifunctionals/Anti fauna
- Binary agents distributed via imported products (Vitamins, Clothing, Food)
- Blast Wave Accelerator - global precision strike "On the Cheap"
- Bio/Chem/Molec./Nano Computing
- Ubiquitous Optical Comms
- Micro/Nano/Ubiquitous Sensors
- BioWeaponry
- Volumetric weaponry
- Cyber/Artificial Life (Beyond AI) -?
- Transoceanic UUV's, UAV's - [4]Boeing's X45 series
- Spherical Submarines to deal with the acoustics issue

To sum up, the best warriors win their battles without waging war – or at least not against themselves.

1.

[http://photos1.blogger.com/blogger/1933/1779/1600/armed\\_robots.jpg](http://photos1.blogger.com/blogger/1933/1779/1600/armed_robots.jpg)

2. <http://nanoatlas.ifs.hr/nano-warfare.html>
3. <http://www.fas.org/man/eprint/FutureWarfare.ppt>
4. [http://en.wikipedia.org/wiki/Boeing\\_X-45](http://en.wikipedia.org/wiki/Boeing_X-45)

474

x

## **Microsoft's OneCare Penetration Pricing Strategy (2006-08-26 14:17)**

[1]

In a previous post, [2]Microsoft in the Information Security Market, I commented on Microsoft's most recent

move into the information security market, and the anti-virus market segment. Moreover, several months earlier I

pointed out [3]5 things Microsoft can do to secure the Internet and why it wouldn't, namely,

- Think twice before reinventing the security industry
- Become accountable, first, in front of itself, than, in front of the its stakeholders
- Reach the proactive level, and avoid the reactive, in respect to software vulnerabilities
- Introduce an internal security oriented culture, or better utilize its workforce in respect to security
- Rethink its position in the security vulnerabilities market

Recently, the much hyped debate on whether Microsoft's Anti Virus would take a piece of the anti virus mar-

ket seem to have[4] finally materialized with the help of basic pricing strategies :

*" Helped by low pricing, Microsoft's Windows Live OneCare landed the number two spot in sales at US stores in*

*its debut month, according to The NPD Group. The antivirus and PC care package nabbed 15.4 per cent of security*

*suite sales at retailers such as Best Buy and Amazon.com, according to NPD's data. The average price was \$29.67,*

*well below Microsoft's list price of \$49.95. Online at Amazon.com, OneCare is available for only \$19.99. "*

Ya-hoo? Not so fast since stats like these exclude the hundreds of licensing deals, co-branding, ISPs affiliation

and resellership positions, as well as shipped-ready PCs with software from the rest of the vendors :

*" Symantec noted that NPD covers retail sales only, and does not include consumer sales through internet ser-*

*vice providers and PC makers, for example. "We just had a record June quarter in consumer sales, said Mike Plante, a marketing director at the company. You can't really draw market share conclusions from the NPD data alone,*

*particularly with just a month of data. "*

I wonder what would Microsoft's strategy consist of by the time their offering reaches the growth stage, and

starts maturing, perhaps bargaining by offering software discounts and one-stop-shop services. I've once pointed out on another [5]anti virus market statistics concern, namely Panda Software's – private company, no SEC or stockholders to bother about – stated earnings right next to the rest of publicly traded companies. My point is that, if Gartner were to offer a better grasp of this vibrant market segment, they'd better have used [6]F-Secure which is a publicly traded anti virus vendor, as it would greatly improve an analysts confidence in the provided data, wouldn't it?

Penetration pricing is all about gaining market share, and Microsoft's case reminds of how [7]RealNetworks

were ready to lose cents on each and every song sold through their digital music service, but to offer, at least temporary, a competitive alternative to iTunes.

Security cannot be bought, a false sense of security can though. Whereas risk exposure and risk mitigation

define a scientific approach going beyond a visionary security management, it's arguable which one dominates, as

marketing and branding often do the job – if (true) advertising does its job, millions of people keep theirs. Case

in point, Symantec which currently has the largest market share – greatly depends on the geographical area and

number of anti virus products included – is indeed the market leader, but it doesn't necessarily mean it offers the

"leading" product. Exactly the opposite, the most popular, available, one that usually comes with Norton's powerful and well known brand offering.

Why wouldn't Microsoft want to [8]license Kaspersky's, F-Secure's or Symantec's technology for instance? Be-

cause that would have been like a Chinese growth syndrome so to speak. The Chinese economy is shifting from a

475

source of raw materials, to an actual manufacturer, a little bit of vertical integration given you have something to offer to the market at a particular moment in time and start counting the new millionaires. The higher proportion

of the business machine you own, the greater the profits at the end of quarter, and with the key regions across the

world still getting online, malware is only going to get more attention from both sides of the front.

From a business point of view, you can twist a user's actual wants so successfully you can make it almost im-

possible to remember what was needed at the first place - long live the sales forces! It is often arguable whether

anti virus software has turned into a commodity the way media players did, but for the end user - the one with the

powerful bandwidth available - price and availability speak for themselves. Controversial to some recent comments

on why [9]the most popular anti virus products don't work, mostly because malware authors are testing their

"releases" on these products, they actually do it on [10]all anti virus products the way pretty much everyone aware is testing suspicious files, or [11]evaluating vendors' response times.

Don't get surprised if next time you buy a cheeseburger, the dude starts explaining the basics of zero day pro-

tection, and offer you a ZIP-based discount if any on an anti virus solution - with up to three licenses for your wired

family. Co-branding, licensing and [12]industry outsiders are on the look for fresh revenues, and with malware

representing the most popular threat as well as security "solution" bought, stay tuned a McDonald's Anti Virus

"on-the-go". Hopefully one using a licensed technology from a vendor with experience and vision.

### **Related posts:**

[13]Look who's gonna cash for evaluating the maliciousness of the Web

[14]Spotting valuable investments in the information security market

[15]Valuing Security and Prioritizing Your Expenditures

[16]Budget Allocation Myopia and Prioritizing Your Expenditures

1.

<http://photos1.blogger.com/blogger/1933/1779/1600/092503.jpg>



2. <http://ddanchev.blogspot.com/2006/05/microsoft-in-information-security.html>
3. <http://ddanchev.blogspot.com/2006/03/5-things-microsoft-can-do-to-secure.html>
4. <http://software.silicon.com/security/0,39024655,39161382,00.htm>
5. <http://ddanchev.blogspot.com/2006/07/anti-virus-signatures-update-it-could.html>
6. <https://europe.f-secure.com/investor-relations/>
7. [http://news.com.com/RealNetworks+slashes+song+prices/2100-1027\\_3-5312143.html](http://news.com.com/RealNetworks+slashes+song+prices/2100-1027_3-5312143.html)
8. [http://news.com.com/AOL+offers+free+antivirus+software/2100-7355\\_3-6102917.html](http://news.com.com/AOL+offers+free+antivirus+software/2100-7355_3-6102917.html)
9. [http://www.zdnet.com.au/blogs/securifythis/soa/Why\\_popular\\_antivirus\\_apps\\_do\\_not\\_work\\_/0,39033341,39264249,00.htm](http://www.zdnet.com.au/blogs/securifythis/soa/Why_popular_antivirus_apps_do_not_work_/0,39033341,39264249,00.htm)
10. <http://www.virustotal.com/>
11. <http://ddanchev.blogspot.com/2006/08/virus-outbreak-response-time.html>
12. <http://www.redherring.com/article.aspx?a=18128>
13. <http://ddanchev.blogspot.com/2006/02/look-whos-gonna-cash-for-evaluating.html>

14. <http://ddanchev.blogspot.com/2006/04/spotting-valuable-investments-in.html>

15. <http://ddanchev.blogspot.com/2006/05/valuing-security-and-prioritizing-your.html>

16. <http://ddanchev.blogspot.com/2006/07/budget-allocation-myopia-and.html>

476

x

x

## **Steganography and Cyber Terrorism Communications (2006-08-26 16:13)**

[1]

Following my previous post on [2]Cyber Terrorism Communications and Propaganda, I'm continuing to

summarize interesting findings on the topic. The use of encryption to ensure the confidentiality of a communication,

be it criminals or terrorists taking advantage of the speed and cheap nature of Internet communications, is often

taken as the de-facto type of communication. I feel that it's [3]steganographic communication in all of its variety that's playing a crucial role in terrorist communications. It's never been about the lack of publicly or even commercially

obtainable steganographic tools, but the ability to know where and what to look for. Here's a brief [4]comment on a

rather hard to intercept communication tool - SSSS - Shamir's Secret Sharing Scheme :

*" No other medium can provide better speed, connectivity, and most importantly anonymity, given it's achieved*

*and understood, and it often is. Plain encryption might seem the obvious answer, but to me it's [5] steganography, having the potential to fully hide within legitimate (at least looking) data flow. Another possibility is the use secret sharing schemes. A bit of a relevant tool that can be fully utilized by any group of people wanting to ensure their*

*authenticity and perhaps everyone's pulse, is [6] SSSS - Shamir's Secret Sharing Scheme. And no, I'm not giving tips, just shredding light on the potential in here! The way botnets of malware can use public forums to get commands, in*

*this very same fashion, terrorists could easily hide sensitive communications by mixing it with huge amounts of public data, while still keeping it secret. "*

Intelligence officials/analysts are often confronted with the difficult task of, should they actively work on scan-

ning the entire public Internet, or single partitions of the known chaos, namely the majority of [7]Islamic/Jihadi

related web sites. Trouble is, it's heck of a short sighted approach, and way too logical one to actually provide results.

Moreover, in all the fuss of terrorists using steganography, even encryption to communicate, the majority of experts

- shooting into the dark - have totally neglected the very concept of disinformation. To be honest, I'm a little bit

surprised on the lack of such, picture the media buzz of a recently found map of key region and encoded messages

embedded in public image, continue with the public institutions raising threat levels, vendors taking advantages of

this "marketing window" when in between, someone gained access to a third-party's E-identity and used to creatively communicate the real message.

It's a public secret that the majority of already obtained [8]Terrorist [9]Training Manuals on the Web give in-

structions on primitive, but IT-centered approaches for anonymity such as encryption, use of proxies, and yes,

steganography as well. Yet another public secret, these very same training manuals are actual copies of unclassified

and publicly obtained Intelligence, Military and Security research documents. Here's a chapter on [10]Secret Writing

and Cipher and Codes. Primitive, but still acting as an indicator of the trend.

[11]

The most comprehensive [12]Scan of the USENET for steganography was conducted back in 2001, pri-

marily because of the [13]post 9/11 debate on the use of steganography by terrorists. Surprisingly, the experiment

didn't find a single hidden image – out of a dictionary based attack on the JSteg and JPHide positive images of course

:

*" After scanning two million images from eBay without finding any hidden messages, we extended the scope of*

*our analysis. A detailed description of the detection framework can be found in [14] Detecting Steganographic Content on the Internet. This page provides details about the analysis of one million images from the [15] Internet Archive's USENET archive. Processing the one million images with stegdetect results in about 20,000 suspicious images. We*

*launched a dictionary attack on the JSteg and JPHide positive images. The dictionary has a size of 1,800,000 words and phrases. The disconcert cluster used to distribute the dictionary attack has a peak performance of roughly 87 GFLOPS. "*

### **Concerns about the invaluable sample :**

- Used primarily USENET as a possible source for images

477

- Excluded music and multimedia files, and the hard to detect while in transmission TCP/IP covert communication channels – information can indeed move with the speed of an error message

- Cannot scan the Dark Web, the one closed behind common crawlers blocking techniques or simple authentication

- Cannot scan what's not public, namely malware-infected hosts, or entire communication platforms hosted on a defaced web server somewhere, temporary communication dead boxes – and while taking about such, [16]free web space providers can provide interesting information given you know where and what to look for as always

The bottom line is that if someone really wants to embed something into a commodity data such as video, picture or an MP3 file, they would. Generating more noise when there's enough of it is on the other hand a smart approach I feel is getting abused all the time. How to deal with the problem? Ensure your [17]ECHELON approaches are capable of detecting the patterns of the majority of public/commercial steganography tools. And according to [18]public sources, that seems to be the case already :

" **R2051 *Steganography Decryption by Distributive Network Attack*** *Develop a distributive network analysis application that can detect, identify, and decrypt steganography in multiple types of files, including commonly used*

*audio, video and graphic file formats. The application must quickly and accurately detect and identify files containing steganography and extract the hidden messages and data from the file. Decryption of any messages or data encoded before the use of a steganography program is not required. The system must allow for easy, low-cost, frequent*

*updating to counter new emerging programs. It must detect, extract, and decrypt messages in any file that has used*

*any currently commercially available steganography programs as well as commonly encountered non-commercial*

*programs. These would include, but are not limited to, the following: **Covert.tcp; dc-Steganograph; EzStego;***

***FFEncode; Gzsteg; Hide 4 PGP; Hide and Seek 4.1; Hide and Seek 5.0; Hide and Seek for Windows 95; jpeg-jsteg;***

***Paranoid, Paranoid1.1.hqx.gz; PGE - Pretty Good Envelope; PGPn123; S-Tools : S-Tools 1.0 (Italy, Finland); S-Tools***

***2.0 (Italy, Finland); S-Tools 3.0 (Italy), Finland); S-Tools 4.0 (Italy, Finland); Scytale; Snow; Stealth, Stealth 2.01***

***; Steganos 1.4; Steganos for Windows 95 and upgrade 1.0a; Stego by John Walker; Stego by Romana Machado;***

***Stegodos; Texto; wbStego; WitnesSoft; and WINSTORM"***

The rest is making sense out of the noise and OSINT approaches for locating the "bad neighborhoods".

Figure courtesy of Bauer 2002 at the FBI's [19]Overview of Steganography for the Computer Forensics Exam-

iner.

1. [http://photos1.blogger.com/blogger/1933/1779/1600/fsc\\_stego\\_kessler\\_fig01.jpg](http://photos1.blogger.com/blogger/1933/1779/1600/fsc_stego_kessler_fig01.jpg)
2. [http://ddanchev.blogspot.com/2006/08/cyber-terrorism-communications-and\\_22.html](http://ddanchev.blogspot.com/2006/08/cyber-terrorism-communications-and_22.html)
3. <http://cse.spsu.edu/jwang/research/security/steganography.pdf>
4. <http://ddanchev.blogspot.com/2005/12/cyberterrorism-dont-stereotype-and-its.html>
5. <http://en.wikipedia.org/wiki/Steganography>
6. <http://point-at-infinity.org/ssss/>
7. [http://tajdeed-list.net/pipermail/pir\\_tajdeed-list.net/2006-June/000092.html](http://tajdeed-list.net/pipermail/pir_tajdeed-list.net/2006-June/000092.html)
8. <http://www.disastercenter.com/terror/>
9. <http://www.thesmokinggun.com/archive/jihadmanual.html>
10. <http://www.thesmokinggun.com/archive/jihad13chap1.html>
11. <http://photos1.blogger.com/blogger/1933/1779/1600/usenet.png>
12. <http://niels.xtdnet.nl/stego/usenet.php>
13. <http://www.usatoday.com/tech/news/2001-02-05-binladen.htm>
14. <http://niels.xtdnet.nl/u/provos/papers/detecting.pdf>



15. <http://www.archive.org/>

16. <http://briefcase.yahoo.com/tcraftp>

17.

<http://www.aclu.org/safefree/nsaspying/23989res20060131.html>

18.

[https://bids.tswg.gov/TSWG/bids.nsf/0/72E38BD12096D4B7852571220065F251/%24FILE/W91CRB-06-T-0032\\_BAA\\_Pkg.](https://bids.tswg.gov/TSWG/bids.nsf/0/72E38BD12096D4B7852571220065F251/%24FILE/W91CRB-06-T-0032_BAA_Pkg.)

[478](#)

[pdf](#)

19.

[http://www.fbi.gov/hq/lab/fsc/backissu/july2004/research/2004\\_03\\_research01.htm](http://www.fbi.gov/hq/lab/fsc/backissu/july2004/research/2004_03_research01.htm)

479



## **Bed Time Reading - Spying on the Bomb (2006-08-27 23:45)**

[1]

Continuing the [2]Bed Time Reading series, and a previous post related to [3]India's Espionage Leaks, this

book is a great retrospective on the [4]U.S Nuclear Intelligence from Nazi Germany to Iran and North Korea.

In-depth review with an emphasis on India's counterintelligence tactics:

***" India's success in preventing U.S. spy satellites from seeing signs of the planned tests days to weeks in ad-***

***vance was matched by its success in preventing acquisition of other types of intelligence.*** India's Intelligence Bureau ran an aggressive counterintelligence program, and the CIA, despite a large station in New Delhi, was unable to

*recruit a single Indian with information about the Vajpayee government's nuclear plans. Instead, the deputy chief*

*of the CIA station in New Delhi was expelled after a botched try at recruiting the chief of Indian counterintelligence operations. Former ambassador Frank Wisner recalled that 'we didn't have... the humans who would have given us*

*an insight into their intentions'." Ambassadors do not keep aloof from the CIA's work, evidently. Their denials are false.*

*NSA's eavesdropping activities did not detect test preparations. "It's a tough problem," one nuclear intelligence expert told investigative journalist Seymour Hersh. **India's nuclear weapons establishment would communicate via***

***encrypted digital messages relayed via small dishes through satellites, using a system known as VSAT (very small***

***aperture terminal), "a two-way version of the system used by satellite television companies"*** . Good show. At the end of the day, Americans admitted that even if they had been better informed, they could not have prevented

*Pokhran II just as they could not deter Pakistan from staging its tests at Chagai. "*

Was the [5]USSR's tactic of helping the enemies of their enemies, thus ruining the Nuclear-club monopoly by

making the A-bomb a public secret, the smartest or dumbest thing they ever did? Monopolies are bad by default,

but balance is precious as the "rush must always be tempered with wisdom". [6]How about a nice game of chess instead?

### **Related resources and posts:**

[7]Nuclear

[8]Who needs nuclear weapons anymore?

[9]North Korea's Strategic Developments and Financial Operations

[10]Japan's Reliance on U.S Spy Satellites and Early Warning Missile Systems

1.

<http://photos1.blogger.com/blogger/1933/1779/1600/20060825001007501.jpg>

2. [http://ddanchev.blogspot.com/2006/08/bed-time-reading-symbian-os-platform\\_12.html](http://ddanchev.blogspot.com/2006/08/bed-time-reading-symbian-os-platform_12.html)

3. <http://ddanchev.blogspot.com/2006/07/indias-espionage-leaks.html>

4. <http://www.hinduonnet.com/fline/stories/20060825001007500.htm>
5. <http://nuclearweaponarchive.org/Russia/Sovwpnprog.html>
6. <http://ddanchev.blogspot.com/2006/03/dvd-of-weekend-war-games.html>
7. <http://del.icio.us/DDanchev/Nuclear>
8. <http://ddanchev.blogspot.com/2006/02/who-needs-nuclear-weapons-anymore.html>
9. <http://ddanchev.blogspot.com/2006/08/north-koreas-strategic-developments.html>
10. <http://ddanchev.blogspot.com/2006/07/japans-reliance-on-us-spy-satellites.html>

480



## **Cyber War Strategies and Tactics (2006-08-28 00:39)**

[1]

Starting from the basic premise that "[2]All warfare is based on

deception", the Cyberspace offers an unprecedented amount of asymmetric power to those capable of using it.

Cyber wars are often perceived as innocent exchange of "virtual shots" between teenage [3]defacement groups,

whereas if one's willing the embrace the rough reality, Hacktivism remains a sub-activity of [4]Cyberterrorism, where

[5]Information Warfare unites all these tactics.

Quality techno-thrillers often imply the notion of [6]future warfare battles done in the [7]virtual realm com-

pared to actual spill of blood and body parts - [8]death is just an upgrade. Coming back to today's Hacktivism

dominated mainstream news space, you may find this paper on [9]Cyberwar Strategy and Tactics - An Analysis of

Cyber Goals, Strategies, Tactics, and Techniques, and the development of a Cyber war Playbook, informative reading :

*" To create a cyberwar playbook, we must first understand the stratagem building blocks or possible moves*

*that are available. It is important to note however that these stratagem building blocks in and of themselves are*

*not strategic. Instead, it is the reasoned application of one or more stratagems in accomplishing higher-level goals that is strategic in nature. We thus need to understand the situations in which the stratagems should be applied and how. We can begin to predict and choose the most effective stratagem for a given situation as we become more*

*experienced. Example stratagems include:*

*Fortify Dodge*

*Deceive Block*

*Stimulate Skirt*

*Condition Monitor*

*Stratagems may also have sub-stratagems. Examples are:*

***Deceive.Chaff — Block.Barricade***

***Deceive.Fakeout — Block.Cutoff***

***Deceive.Conceal — Monitor.Eavesdrop***

***Deceive.Feint — Monitor.Watch***

***Deceive.Misinform — Monitor.Follow***

*These stratagems are very high level and can be supported through many tactical means. Each building block*

*defines a stratagem and contains one or more possible tactical implementations for that stratagem, including re-*

*quirements, goals that may be satisfied using the stratagem, caveats, example uses, and possible countermeasures. "*

No matter the NCW doctrine, UAVs intercepting or hijacking signals, "[10]shock and awe" still dazzles the ma-

jority of prone to be abused by cheap [11]PSYOPS masses of "individuals".

### **Related resources and posts:**

481

[12]Network Centric Warfare basics back in 1995

[13]Information Warfare

[14]Cyber Warfare

[15]Who's Who in Cyber Warfare?

[16]North Korea's Cyber Warfare Unit 121

[17]Hacktivism Tensions - Israel vs Palestine Cyberwars

[18]Achieving Information Warfare Dominance Back in 1962

1.

[http://photos1.blogger.com/blogger/1933/1779/1600/VR\\_Cyberwarfare\\_Simulation.jpg](http://photos1.blogger.com/blogger/1933/1779/1600/VR_Cyberwarfare_Simulation.jpg)

2. <http://www.quotationspage.com/quote/34335.html>

3.

<http://photos1.blogger.com/blogger/1933/1779/1600/dtool-1.0.png>

4. <http://ddanchev.blogspot.com/2006/05/techno-imperialism-and-effect-of.html>

5.

[http://photos1.blogger.com/blogger/1933/1779/1600/information\\_warfare.1.gif](http://photos1.blogger.com/blogger/1933/1779/1600/information_warfare.1.gif)

6.

<http://www.airpower.maxwell.af.mil/airchronicles/battle/chp6.html>

7.

[http://www.findarticles.com/p/articles/mi\\_m0EPF/is\\_n8\\_v95/ai\\_17459300](http://www.findarticles.com/p/articles/mi_m0EPF/is_n8_v95/ai_17459300)

8. <http://www.cyberpunkreview.com/cyberpunked-living/dose-interview-with-gene-generations-pearry-reginald-te>



[o/](#)

9.

[http://www.cyberdefenseagency.com/publications/Cyberwar\\_Strategy\\_and\\_Tactics.pdf](http://www.cyberdefenseagency.com/publications/Cyberwar_Strategy_and_Tactics.pdf)

10. [http://en.wikipedia.org/wiki/Shock\\_and\\_awe](http://en.wikipedia.org/wiki/Shock_and_awe)

11. <http://del.icio.us/DDanchev/PSYOPS>

12.

<http://www.time.com/time/magazine/article/0,9171,983318,00.html>

13. <http://del.icio.us/DDanchev/InformationWarfare>

14. <http://del.icio.us/DDanchev/Cyberwarfare>

15. <http://ddanchev.blogspot.com/2006/05/whos-who-in-cyber-warfare.html>

16. <http://ddanchev.blogspot.com/2006/07/north-koreas-cyber-warfare-unit-121.html>

17. <http://ddanchev.blogspot.com/2006/07/hacktivism-tensions-israel-vs.html>

18. <http://ddanchev.blogspot.com/2006/08/achieving-information-warfare.html>

482

**2.9**

**September**

483



## **The Walls and Lamps are Listening (2006-09-02 00:13)**

[1]

And so are the hardware implanted "covert operatives".

1.

[http://photos1.blogger.com/blogger/1933/1779/1600/covert\\_operative.jpg](http://photos1.blogger.com/blogger/1933/1779/1600/covert_operative.jpg)

484



## **The Biggest Military Hacks of All Time (2006-09-02 00:21)**

[1]

The [2]biggest military hack of all time, the [3]Pentagon hacker, the [4]NASA hacker - hold your breath, it's

another media hype or traffic acquisition headline strategy by the majority of online media sites. Who else are

we missing? The NASA port scanner, the true walking case study on tweaking NMAP for subconscious espionage

purposes, the [5]CIA IRC junkies that managed to talk them into talking with "them", and Bozo the clown chased by the [6]Thought Police for his [7]intentions.

Great examples of buzz generating, deadline-centered news articles you can always amuse yourself with, and

feel sorry for the lack of insightful perspectives nowadays – I’m slowly compiling a list of best of the best news items ever, so let there be less [8]intergalactic security statements, and less [9]flooding web sites with Hezbollah data

stories.

In case you’ve somehow missed [10]Gary McKinnon’s story, don’t you worry as you haven’t missed anything

spectacular, besides today’s flood of reporters with claimed prehistoric IT security experience – you must make

the difference between a reporter, a journalist, and a barking dog thought. Perhaps the only objective action done

by an industry representative was the [11]Sophos survey on Gary McKinnon. It would be much more credible to

differentiate the severity of the hack, depending on which military or government network was actually breached,

don’t just go where the wind blows, barely reporting, where’s YOUR opinion if ANY?

Was it the **NSANet**, the [12]Joint Worldwide Intelligence Communications System [JWICS], the [13]Secret Inter-

net Protocol Router Network (SIPRNET), or the [14]Unclassified but Sensitive Internet Protocol Router Network

(NIPRNet) actually breached?

Moreover, were the following real-life examples a paintball game or something :

### **- [15]Solar SunRise**

*" SOLAR SUNRISE was a series of DoD computer network attacks which occurred from 1-26 February 1998. The attack pattern was indicative of a preparation for a follow-on attack on the DII. DoD unclassified networked computers*

*were attacked using a well-known operating system vulnerability. The attackers followed the same attack profile: (a) probing to determine if the vulnerability exists, (b) exploiting the vulnerability, (c) implanting a program (sniffer) to gather data, and (d) returning later to retrieve the collected data."*

### **- [16]Dutch hackers during the Gulf War**

*" At least one penetrated system directly supported U.S. military operations in Operation Desert Storm prior to the Gulf War. They copied or altered unclassified data and changed software to permit future access. The hackers were*

*also looking for information about nuclear weapons. Their activities were first disclosed by Dutch television when*

*camera crews filmed a hacker tapping into what was said to be U.S. military test information. "*

### **- [17]The Case Study: Rome Laboratory, Griffiss Air Force Base**

*" However, events really began in 1994, when the two young men broke into an Air Force installation known as*

*Rome Labs, a facility at the now closed Griffiss Air Force Base, in New York. This break-in became the centerpiece*

*of a Government Accounting Office report on network intrusions at the Department of Defense in 1996 and also*

*constituted the meat of a report entitled "Security and Cyberspace" by Dan Gelber and Jim Christy, presented to the Senate Permanent Subcommittee on Investigations during hearings on hacker break-ins the same year. It is*

*interesting to note that Christy, the Air Force Office of Special Investigations staffer/author of this report, was never at Rome while the break-ins were being monitored. "*

#### **- [18]Moonlight Maze**

485

*" It was claimed that these hackers had obtained large stores of data that might include classified naval codes and information on missile guidance systems, though it was not certain that any such information had in fact been compromised. "*

#### **- [19]Titan Rain**

*" Titan Rain hackers have gained access to many U.S. computer networks, including those at Lockheed Martin, Sandia National Laboratories, Redstone Arsenal, and NASA. "*

#### **- [20]Chinese hackers who supposedly downloaded 10 to 20 terabytes from the NIPRNet – it's like I love you**

from 1 to 50, and you?

From another perspective, the biggest military hack doesn't have to come from the outside, but from the in-

side, as [21]soldiers are easily losing their USB sticks on the field. Breaching the SIPRnet from the outside would be a

good example of a big military hack, but then again, [22]insiders are [23]always there to "take care".

If [24]Gary McKinnon did the biggest military hack of all time, why do I still hear Bozo singing - ta ta tararata

ta ta rara tata.

### **UPDATE:**

Related posts you might also find informative - [25]North Korea's Cyber Warfare Unit 121, [26]Techno imperialism

and the effect of Cyber terrorism, [27]Cyber War Strategies and Tactics, the rest you can [28]Google. Surprised to

come across the post at [29]Meneame.net too.

1.

<http://photos1.blogger.com/blogger/1933/1779/1600/wargames.jpg>

2. [http://www.google.com/search?](http://www.google.com/search?hl=en&lr=&q=biggest+military+hack)

[hl=en&lr=&q=biggest+military+hack](http://www.google.com/search?hl=en&lr=&q=biggest+military+hack)

3. [http://www.google.com/search?](http://www.google.com/search?hl=en&lr=&q=pentagon+hacker)

[hl=en&lr=&q=pentagon+hacker](http://www.google.com/search?hl=en&lr=&q=pentagon+hacker)

4. [http://www.google.com/search?](http://www.google.com/search?hl=en&lr=&q=NASA+hacker)

[hl=en&lr=&q=NASA+hacker](http://www.google.com/search?hl=en&lr=&q=NASA+hacker)

5.

[http://www.theregister.co.uk/2000/12/01/cia\\_sacks\\_four\\_in\\_secret/](http://www.theregister.co.uk/2000/12/01/cia_sacks_four_in_secret/)

6. [http://en.wikipedia.org/wiki/Thought\\_Police](http://en.wikipedia.org/wiki/Thought_Police)
7. <http://www.zone-h.org/content/view/14097/28/>
8. <http://ddanchev.blogspot.com/2006/07/intergalactic-security-statement.html>
9. <http://www.upi.com/NewsTrack/view.php?StoryID=20060831-015318-9708r>
10. [http://en.wikipedia.org/wiki/Gary\\_McKinnon](http://en.wikipedia.org/wiki/Gary_McKinnon)
11. <http://www.sophos.com/pressoffice/news/articles/2006/07/mckinnon.html>
12. <http://www.fas.org/irp/program/disseminate/jwics.htm>
13. <http://www.fas.org/irp/program/disseminate/siprnet.htm>
14. <http://en.wikipedia.org/wiki/NIPRNet>
15. <http://www.globalsecurity.org/military/ops/solar-sunrise.htm>
16. [http://www.wasc.noaa.gov/wrso/security\\_guide/hacking.htm](http://www.wasc.noaa.gov/wrso/security_guide/hacking.htm)
17. <http://www.soci.niu.edu/~crypt/other/afosi.htm>
18. [http://en.wikipedia.org/wiki/Moonlight\\_Maze](http://en.wikipedia.org/wiki/Moonlight_Maze)
19. [http://en.wikipedia.org/wiki/Titan\\_Rain](http://en.wikipedia.org/wiki/Titan_Rain)
20. [http://www.gcn.com/print/25\\_25/41716-1.html](http://www.gcn.com/print/25_25/41716-1.html)
21. [http://news.bbc.co.uk/2/hi/south\\_asia/4905052.stm](http://news.bbc.co.uk/2/hi/south_asia/4905052.stm)

22. <http://ddanchev.blogspot.com/2005/12/insiders-insights-trends-and-possible.html>
23. [http://en.wikipedia.org/wiki/Pentagon\\_Papers](http://en.wikipedia.org/wiki/Pentagon_Papers)
24. <http://www.spy.org.uk/freegary/>
25. <http://ddanchev.blogspot.com/2006/07/north-koreas-cyber-warfare-unit-121.html>
26. <http://ddanchev.blogspot.com/2006/05/techno-imperialism-and-effect-of.html>
27. <http://ddanchev.blogspot.com/2006/08/cyber-war-strategies-and-tactics.html>

486

28. <http://www.google.com/search?hl=en&q=site%3Addanchev.blogspot.com+cyber+warfare>
29. <http://meneame.net/story/the-biggest-military-hacks-of-all-time>

487



### **Chinese Hackers Attacking U.S Department of Defense Networks (2006-09-03 20:58)**

[1]

This may prove to be an [2]informative forum, and I feel that the quality of the questions and the discussion

faciliator's insights in the topic – as a matter of fact GCN has proven a reliable source on the topic – will be my



benchmark for a provocative many-to-many discussion.

### **Here are my questions :**

- Despite PRC's growing Internet population and military thinking greatly emphasizing on pros of information/cyber

warfare – the concepts copied from the U.S in between Sun Tzu's mode of thinking and attitude may indeed prove

a dangerous combination – I find it a bit more [3]complex issue as: " *Let's don't forget the use and abuse of island hopping points fueling further tensions in key regions and abusing the momentum itself, [4] physically locating a network device in the future IPv6 network space is of key interest to all parties.* " China's growing Internet population results in lots of already infected malware hosts that could easily act as stepping stones by third-parties.

My point : **Is it a geopolitical tension engineering, or an active doctrine already in implementation?**

- If it's indeed a Red Storm Rising, what's North Korea's place in the situation, could it be North Korea engi-

neering and impersonating China's cyber forces thus helping the enemies of its enemies?

- What significant is the threat from actual PRC's cyber warfare divisions, compared to utilizing the massess of

script kiddies and promoting – and not prosecuting attacks on foreign adversaries – hacking activities? Script

kiddies pretending to be l33t, or cyber warfare divisions using retro techniques to disinform on the actual state of

military preparedness? The rise of intellectual property theft worms that I [5]discussed, especially [6]Myfip has

been connected with the Titan Rain attacks on military networks, but this can be so easily engineered to point out wherever you want it to :

*" Myfip doesn't spread back out via the Simple Mail Transfer Protocol (SMTP). "There is no code in the worm to do this," the report said. "From certain key headers in the message, we can tell that the attachment was sent directly to [users]." One element that stands out is that Myfip e-mails always have one of two X-Mailer headers: X-Mailer: FoxMail 4.0 beta 2 [cn] and X-Mailer: FoxMail 3.11 Release [cn]. Also, it always uses the same MIME*

*boundary tag: \_NextPart\_2rfkindysadvnqw3nerasdf. "These are signs of a frequently-seen Chinese spamtool...", the report said. Stewart said his team was easily able to trace the source of Myfip and its variants. "They barely make any effort to cover their tracks," he said. **And in each case, the road leads back to China. Every IP address involved***

***in the scheme, from the originating SMTP hosts to the "document collector" hosts, are all based there, mostly in***

***the Tianjin province. "***

- Where does the real threat come from exactly? Hackers reading unclassified but sensitive clerk's emails thus

exposing the network's design and gathering intelligence for the future "momentum", or the use of [7]PSYOPS

online? How is the second measured as a key foundation for successful information warfare battle?

- Is it a state sponsored espionage and cyber warfare practices, or mainland [8]hacktivists, perhaps even hired third party guns?

Image courtesy of Chinese hackers diversifying their attacks and causing more noise during the [9]U.S/China cyber

skirmish.

### **Related resources and posts:**

[10]Cyber Warfare

488

[11]Information Warfare

[12]Hacktivism Tensions - Israel vs Palestine Cyberwars

[13]Cyber War Strategies and Tactics

[14]Who's who in Cyber Warfare?

1.

[http://photos1.blogger.com/blogger/1933/1779/1600/QFZ\\_email\\_flooder\\_hacktivism.2.jpg](http://photos1.blogger.com/blogger/1933/1779/1600/QFZ_email_flooder_hacktivism.2.jpg)

2. [http://www.gcn.com/forum/qna\\_forum/41835-1.html](http://www.gcn.com/forum/qna_forum/41835-1.html)

3. <http://ddanchev.blogspot.com/2006/07/north-koreas-cyber-warfare-unit-121.html>

4. <http://www.caidda.org/~yoshi/KoBrCl05PDF-hires.pdf>

5. <http://www.linuxsecurity.com/docs/malware-trends.pdf>
6. [http://searchsecurity.techtarget.com/originalContent/0,289142,sid14\\_gci1120855,00.html](http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1120855,00.html)
7. <http://ddanchev.blogspot.com/2006/02/hacktivism-tensions.html>
8. <http://del.icio.us/DDanchev/Hacktivism>
9. [http://www.cmc.gov.my/what\\_we\\_do/ins/IndustryTalk/Presentation1.pdf](http://www.cmc.gov.my/what_we_do/ins/IndustryTalk/Presentation1.pdf)
10. <http://del.icio.us/DDanchev/Cyberwarfare>
11. <http://del.icio.us/DDanchev/InformationWarfare>
12. <http://ddanchev.blogspot.com/2006/07/hacktivism-tensions-israel-vs.html>
13. <http://ddanchev.blogspot.com/2006/08/cyber-war-strategies-and-tactics.html>
14. <http://ddanchev.blogspot.com/2006/05/whos-who-in-cyber-warfare.html>

489



**Zero Day Initiative Upcoming Zero Day Vulnerabilities (2006-09-04 21:03)**

[1]

Details on a dozen of "[2]upcoming zero day vulnerabilities" are emerging from [3]TippingPoint's Zero Day

Initiative :

*" Over the past year, the most resounding suggestion from our Zero Day Initiative researchers was to add more transparency to our program by publishing the pipeline of vendors with pending zero day vulnerabilities. The following is a list of vulnerabilities discovered by researchers enrolled in the Zero Day Initiative that have yet to be publicly disclosed.*

*The affected vendor has been contacted on the specified date and while they work on a patch for these vulnerabilities, TippingPoint customers are protected from exploitation by IPS filters delivered ahead of public disclosure. A list of*

*[4] published advisories is also available. "*

Note the time from vulnerability reporting to patch on some vendors:

ZDI-CAN-041 – Computer Associates – High – 2006.04.07,  
**144 days ago**

ZDI-CAN-042 – Adobe – High – 2006.04.07, **144 days ago**

ZDI-CAN-046 – Computer Associates – High – 2006.04.07,  
**144 days ago**

ZDI-CAN-061 – Microsoft – High – 2006.06.14, **76 days ago**

Don't be in a hurry to blame the vendors, as in between having to deal with these zero day vulnerabilities, they're

all providing patches to fix the emerging ones, that is those who get the highest publicity and make the headlines so

actively that there's no other way but dedicating product development time to quality assurance. Keep in mind that,

even though vendors are still working on fixing these, apparently TippingPoint's IPS customers are protected - they're

aware of these exploits. Excluding the vendor dependability issue, and the fact that ZDI is indisputably turning into a

HR-on-demand think-tank for vulnerability research, I discussed some of the issues regarding the possible motivation

of the vulnerability intermediaries and what to keep in mind in a previous [5]post :

- *trying to attract the most talented researchers, instead of having them turn to the dark side? I doubt they are that much socially oriented, but still it's an option?*

- *ensuring the proactive security of its customers through first notifying them, and then them and then the general public?*

*That doesn't necessarily secures the Internet, and sort of provides the clientele with a false feeling of security, "what if" a (malicious) vulnerability researcher doesn't cooperate with iDefense, and instead sells an 0day to a competitor?*

*Would the vendor's IPS protect against a threat like that too?*

- *fighting against the permanent opportunity of another 0day, gaining only a temporary momentum advantage?*

*- improving the company's clients list through constant collaboration with leading vendors while communication a vulnerability in their software products?*

Diversify your infrastructure to minimize the damages due to zero day outbreaks, ensure end users are privileged as

much as they need, do your homework, camouflage and implement early warning systems/decoys, and yes, keep

track of your assets and ensure they're already protected from what's known to be their vulnerability. Responsible

disclosure is the socially oriented approach, trouble is the Internet itself is a capitalistic society with basic market forces.

### **Related posts:**

[6]Was the WMF vulnerability purchased for \$4000?!

[7]0bay - how realistic is the market for security vulnerabilities?

[8]Scientifically Predicting Software Vulnerabilities

1.

<http://photos1.blogger.com/blogger/1933/1779/1600/zdi.1.jpg>

2. <http://ddanchev.blogspot.com/2006/05/delaying-yesterdays-0day-security.html>

3.

[http://www.zerodayinitiative.com/upcoming\\_advisories.html](http://www.zerodayinitiative.com/upcoming_advisories.html)

4. <http://www.zerodayinitiative.com/advisories.html>

5. <http://ddanchev.blogspot.com/2006/03/wheres-my-0day-please.html>

490

6. <http://ddanchev.blogspot.com/2006/01/was-wmf-vulnerability-purchased-for.html>

7. <http://ddanchev.blogspot.com/2005/12/0bay-how-realistic-is-market-for.html>

8. <http://ddanchev.blogspot.com/2006/07/scientifically-predicting-software.html>

491



## **Stealth Satellites Developments Source Book (2006-09-04 23:40)**

[1]

You can't [2]hijack, intercept or hide from what you don't see or don't know it's there, and stealthy satellites

are going to get even more attention in the ongoing [3]weaponization of space and the emerging [4]space warfare

arms race. Here's a [5]huge compilation of articles and news items related to the development of stealthy satellites.

An excerpt from an article within :

*" The United States is building a new generation of spy satellites designed to orbit undetected, in a highly classified*



*program that has provoked opposition in closed congressional sessions where lawmakers have questioned*

*its necessity and rapidly escalating price, according to U.S. officials. The previously undisclosed effort has almost doubled in projected cost – from \$5 billion to nearly \$9.5 billion, officials said. The National Reconnaissance Office, which manages spy satellite programs, has already spent hundreds of millions of dollars on the program, officials said.*

*The stealth satellite, which would probably become the largest single-item expenditure in the \$40 billion intelligence budget, is to be launched in the next five years and is meant to replace an existing stealth satellite, according to officials. **Non-stealth satellites can be tracked and their orbits can be predicted, allowing countries to attempt***

***to hide weapons or troop movements on the ground when they are overhead.** Opponents of the new program,*

*however, argue that the satellite is no longer a good match against today's adversaries: terrorists seeking small*

*quantities of illicit weapons, or countries such as North Korea and Iran, which are believed to have placed their*

*nuclear weapons programs underground and inside buildings specifically to avoid detection from spy satellites and*

*aircraft. "*

### **Issues to keep in mind :**

- pre-launch leak in today's OSINT world

- synchronization with HUMINT, SIGINT, OSINT gathered data to avoid deception, some developments are right there

under your nose

- [6]amateur radio and satellite enthusiasts outwitting the stealthiness as it always happens

- win-win IMINT sharing between countries can often cover the full spectrum, dependability is of course an issue

### **Related resources and posts:**

[7]Defense

[8]Satellite

[9]Japan's Reliance on U.S Spy Satellites and Early Warning Missile Systems

[10]Open Source North Korean IMINT Reloaded

1.

[http://photos1.blogger.com/blogger/1933/1779/1600/rec\\_satellite.jpg](http://photos1.blogger.com/blogger/1933/1779/1600/rec_satellite.jpg)

2. <http://ddanchev.blogspot.com/2006/08/anti-satellite-weapons.html>

3. <http://ddanchev.blogspot.com/2006/07/weaponizing-space-and-emerging-space.html>

4. <http://ddanchev.blogspot.com/2006/03/is-space-warfare-arms-race-really.html>

5. <http://www.fas.org/spp/military/program/track/stealth.pdf>

6. <http://www.stoff.pl/>

7. <http://del.icio.us/DDanchev/Defense>
8. <http://del.icio.us/DDanchev/Satellite>
9. <http://ddanchev.blogspot.com/2006/07/japans-reliance-on-us-spy-satellites.html>
10. <http://ddanchev.blogspot.com/2006/07/open-source-north-korean-imint.html>

492



## **Benefits of Open Source Intelligence - OSINT (2006-09-05 00:49)**

[1]

Surprisingly, Forbes, the homepage for the world's business leaders – and

wannabe ones – has a well written article on [2]Open Source Intelligence you might find informative :

*" How can we use this to reform intelligence? I suggest we create a national Open Source Agency. Half of the*

*money earmarked for the agency would go toward traditional intelligence work. The other half would provide for*

*50 state-wide Citizen Intelligence Networks, including a 24/7 watch center, where citizens can both obtain and input information. We could establish new emergency intelligence phone numbers–think 119 instead of 911–allowing any*

*housewife, cab driver or delivery boy to contribute to our national security. All they have to do is be alert, and if they see something, take a cell phone photograph and send it in with a text message. If three different people notice the same suspicious person taking photographs of a nuclear plant, for instance, it could be hugely important. The system could even evolve to automatically mobilize emergency workers or warn citizens. Imagine if after people alerted*

*the network about a roadside car bomb, it automatically sent text messages to every phone in the immediate area, warning people to stay away. "*

Collective intelligence, wisdom of crowds – [3]Web users were supposed to virtually patrol the U.S border

once – all is driving Web 2.0, trouble is so is paranoia, and all paranoid people need is a platform to spread it further, but the article emphasises on how educated citizens can be the best defense. [4]The benefits of OSINT according the

CIA themselves are based on :

***Speed:*** *When a crisis erupts in some distant part of the globe, in an area where established intelligence assets are thin, intelligence analysts and policymakers alike will often turn first to the television set and Internet.*

***Quantity:*** *There are far more bloggers, journalists, pundits, television reporters, and think-tankers in the world than there are case officers. While two or three of the latter may, with good agents, beat the legions of open*

*reporters by their access to secrets, the odds are good that the composite bits of information assembled from the*

*many can often approach, match, or even surpass the classified reporting of the few.*

**Quality:** *As noted above, duped intelligence officers at times produce reports based on newspaper clippings*

*and agent fabrications. Such reports are inferior to open sources untainted by agent lies.*

**Clarity:** *An analyst or policymaker often finds even accurate HUMINT a problem. For example, when an offi-*

*cer of the CIA's Directorate of Intelligence (DI), reads a report on a foreign leader based on "a source of unproven reliability," or words to that effect, the dilemma is clear. Yet, the problem remains with a report from a "reliable source." Who is that? The leader's defense minister? The defense minister's brother? The mistress of*

*the defense minister's brother's cousin? The DI analyst will likely never know, for officers of the Directorate of*

*Operations (DO) closely guard their sources and methods. This lack of clarity reportedly contributed, for example,*

*to the Iraqi WMD debacle in 2002-03. The DO reportedly described a single source in various ways, which may*

*have misled DI analysts into believing that they had a strong case built on multiple sources for the existence of Iraqi weapons of mass destruction. With open information, sources are often unclear. With secrets, they almost always are.*

***Ease of use:*** *Secrets, hidden behind classifications, compartments, and special access programs, are difficult to share with policymakers and even fellow intelligence officers. All officials may read OSINT.*

***Cost:*** *A reconnaissance satellite, developed, launched, and maintained at a cost of billions of dollars, can provide images of a weapons factory's roof or a submarine's hull. A foreign magazine, with an annual subscription cost*

*of \$100, may include photographs of that factory's floor or that submarine's interior*

Meanwhile, [5]Intelligence analysts are putting efforts into [6]sharing their data, [7]data mining the web [8]and social networking sites which is both, cost-effective and can greatly act as an early warning system for important events.

Despite technological innovations, a blogger in an adversary's country can often unknowingly act as a HUMINT

source of first-hand information – looking for [9]democracy minded individuals breaking through regimes through

malware is yet another possibility. [10]Tracking down terrorist propaganda and [11]communications on the Internet

has already reached the efficiency level mainly because of the use of open source intelligence and [12]web crawling

the known [13]bad neighborhoods ever [14]since 2001.

### **Related resources and posts:**

[15]Intelligence

[16]OSINT

[17]IP cloaking and competitive intelligence/disinformation

[18]Terrorist Social Network Analysis

1. [http://photos1.blogger.com/blogger/1933/1779/1600/info\\_sharing.jpg](http://photos1.blogger.com/blogger/1933/1779/1600/info_sharing.jpg)
2. [http://www.forbes.com/2006/04/15/open-source-intelligence\\_cx\\_rs\\_06slate\\_0418steele.html](http://www.forbes.com/2006/04/15/open-source-intelligence_cx_rs_06slate_0418steele.html)
3. <http://news.bbc.co.uk/1/hi/world/americas/5040372.stm>
4. [https://www.cia.gov/csi/studies/Vol49no2/reexamining\\_the\\_distinction\\_3.htm](https://www.cia.gov/csi/studies/Vol49no2/reexamining_the_distinction_3.htm)
5. <http://ddanchev.blogspot.com/2006/08/analyzing-intelligence-analysts.html>
6. <http://www.washingtonpost.com/wp-dyn/content/graphic/2006/08/09/GR2006080900190.html>
7. <http://www.newscientist.com/article/mg19025556.200?DCMP=NLC-nletter&nsref=mg19025556.200>
8. <http://www.defenselink.mil/transformation/articles/2006-06/ta062906b.html>
9. <http://www.ravantivirus.com/virus/showvirus.php?v=216>
10. <http://ddanchev.blogspot.com/2006/06/tracking-down-internet-terrorist.html>
11. [http://ddanchev.blogspot.com/2006/08/cyber-terrorism-communications-and\\_22.html](http://ddanchev.blogspot.com/2006/08/cyber-terrorism-communications-and_22.html)

12.

[http://ai.arizona.edu/research/terror/publications/ISI\\_Allab\\_submission\\_final.pdf](http://ai.arizona.edu/research/terror/publications/ISI_Allab_submission_final.pdf)

13. [http://tajdeed-list.net/pipermail/pir\\_tajdeed-list.net/2006-June/000092.html](http://tajdeed-list.net/pipermail/pir_tajdeed-list.net/2006-June/000092.html)

14.

<http://www.epic.org/privacy/choicepoint/acxiominternet.pdf>

15. <http://del.icio.us/DDanchev/Intelligence>

16. <http://del.icio.us/DDanchev/OSINT>

17. <http://ddanchev.blogspot.com/2005/12/ip-cloaking-and-competitive.html>

18. <http://ddanchev.blogspot.com/2006/05/terrorist-social-network-analysis.html>

494



## **HP Spying on Board of Directors' Phone Records (2006-09-06 17:33)**

[1]

Whether a [2]healthy paranoia, or a series of detailed leaks to the press on HP's future long term strategy,

it prompted [3]HP's chair woman to hire experts that obtained access to the call histories of its board of directors'

home and cell phone communications thinking possible [4]insiders :



*" Last January, the online technology site CNET published an article about the long-term strategy at HP, the company ranked No. 11 in the Fortune 500. While the piece was upbeat, it quoted an anonymous HP source and contained information that only could have come from a director. HP's chairwoman, Patricia Dunn, told another director she wanted to know who it was; she was fed up with ongoing leaks to the media going back to CEO Carly Fiorina's tumultuous tenure that ended in early 2005. According to an internal HP e-mail, Dunn then took the extraordinary step of authorizing a team of independent electronic-security experts to spy on the January 2006 communications of the other 10 directors-not the records of calls (or e-mails) from HP itself, but the records of phone calls made from personal accounts. That meant calls from the directors' home and their private cell phones. "*

### **The case highlights that :**

- Classification programs type of protection is rarely utilized of companies aiming to balance the trade off of achieving productivity while keep the left hand not knowing what the right is doing when it's necessary - remember it's [5]the

HP way and the management by open spaces that made the company what it is today

- Didn't bother to disinform suspicious parties and decoy them, thus limiting the circle of "suspects"

- Didn't build transparency into the process and that's just starting to make impact

- It's shortsighted thinking on whether the information defined as leaked wasn't [6]easy to construct through public sources, or that the internal changes weren't already spotted by industry analysts

- They're about to lose their current talented HR, and the one that was about to join HP. Soft HR dollars are on

stake, as I can imagine what will be the faith of a HP blogger if that's how board of directors members threat each other Here's the [7]article of question, and what provoked this to happen :

**" According to the source, HP is considering making more acquisitions in the infrastructure software arena.**

*Those acquisitions would include security software companies, storage software makers and software companies*

*that serve the blade server market. The acquisitions would dovetail with HP's growth plans for its Technology*

*Systems Group, which has already bought companies such as [8] ApplQ for storage management. Hurd has previously said market trends indicate a movement away from mainframe computers and a shift to blade servers, as well as*

*virtualized storage. HP is likely to follow those trends. Meanwhile, in HP's Imaging & Printing Group, the long-term plan to develop commercial printers is likely to continue.*

*"We want to develop the next Heidelberg press," **the source***

***said. Of course, HP said basically [9] the same thing back in 2002. "***

In a previous post, [10]When Financial and Information Security Risks are Supposed to Intersect, I commented

on Morgan Stanley's case of knowing who did what, and the growing enforcement of security policies, thus firing

employees violating them by forwarding sensitive information to home email accounts. But with the media trying to

generate buzz while keeping it objective by mentioning its "sources" and putting the emphasise on "inside company source" no wonder HP is thinking insiders, rather than talkative directors who when asked does the Sun come out in

the morning and goes down in the evening, would think twice before answering – and question the question itself!

[11]Privacy monster courtesy of the EFF.

### **Related resources and posts:**

[12]Espionage

[13]Insider

495

[14]Wiretapping

[15]Surveillance

[16]Smoking Emails

[17]Insider Competition in the Defense Industry

[18]Espionage Ghosts Busters

1.  
<http://photos1.blogger.com/blogger/1933/1779/1600/ouch.4.jpg>
2. <http://ddanchev.blogspot.com/2006/05/healthy-paranoia.html>
3. <http://www.msnbc.msn.com/id/14687677/site/newsweek/>
4. <http://ddanchev.blogspot.com/2005/12/insiders-insights-trends-and-possible.html>
5. [http://www.hpalumni.org/hp\\_way.htm](http://www.hpalumni.org/hp_way.htm)
6. <http://ddanchev.blogspot.com/2006/09/benefits-of-open-source-intelligence.html>
7. [http://news.com.com/HP+outlines+long-term+strategy/2100-1014\\_3-6029519.html](http://news.com.com/HP+outlines+long-term+strategy/2100-1014_3-6029519.html)
8.  
[http://news.com.com/HP+to+acquire+identity+management+firm/2100-1014\\_3-5976834.html?tag=nl](http://news.com.com/HP+to+acquire+identity+management+firm/2100-1014_3-5976834.html?tag=nl)
9.  
[http://news.com.com/HP+pressing+for+more+printer+business/2100-1001\\_3-963469.html?tag=nl](http://news.com.com/HP+pressing+for+more+printer+business/2100-1001_3-963469.html?tag=nl)
10. <http://ddanchev.blogspot.com/2006/07/when-financial-and-information.html>
11. <http://www.eff.org/Privacy/Monsters/>

12. <http://del.icio.us/DDanchev/Espionage>
13. <http://del.icio.us/DDanchev/Insider>
14. <http://del.icio.us/DDanchev/Wiretapping>
15. <http://del.icio.us/DDanchev/Surveillance>
16. <http://ddanchev.blogspot.com/2006/02/smoking-emails.html>
17. <http://ddanchev.blogspot.com/2006/05/insider-competition-in-defense.html>
18. <http://ddanchev.blogspot.com/2006/05/espionage-ghosts-busters.html>

496



### **Hezbollah's use of Unmanned Aerial Vehicles - UAVs (2006-09-06 19:36)**

[1]

According to the common wisdom, terrorists – or let's just say contradictory political fractions – weren't

supposed to be capable of owning the using [2]unmanned aerial vehicles in war conflicts, but be only able to wage

guerilla warfare thus balancing the unequal forces in a conflict. Seems like [3]Hezbollah are indeed capable of owning

and using UAVs, as Israel recently shot down yet another one :

*" Israeli aircraft shot down an unmanned spy plane launched by the Lebanese guerrilla group Hizbollah as it entered Israeli territory on Monday, the Israeli army said. The drone was spotted by the air force's monitoring unit and fighter planes were scrambled to intercept it, an Israeli military spokesman said. The spokesman said a fighter plane shot the drone down 10 km (six miles) off Israel's coast, northwest of the city of Haifa. "The current assessment is that it was headed further south, we do not know exactly for what purpose," the spokesman said. An Israeli military source added that it was an Iranian-made drone with a range of about 150 km. "*

Go through an in-depth post at [4]DefenseTech, and **Eugene Miasnikov's** report on [5]Threat of Terrorism Using Unmanned Aerial Vehicles: Technical Aspects, which :

*" assesses the technical possibility of UAV use as a delivery means for terrorists. The analysis shows that such a threat does exist and that it will grow. The author also considers areas that require higher attention from government agencies. This report is also targeted at the Russian public. Terrorist activity can be prevented only through the coordinated efforts of the government and civil society. The government cannot efficiently fight terrorists without the active involvement of the population. The first step toward creating such an alliance is to recognize the threat and its potential consequences. "*

So what's next once reconnaissance is taken care of and timely intelligence gathered? [6]UCAVs in the long

term, of course. Nothing's impossible, the impossible just takes a little while!

1. [http://photos1.blogger.com/blogger/1933/1779/1600/predator\\_01.jpg](http://photos1.blogger.com/blogger/1933/1779/1600/predator_01.jpg)

2. [http://en.wikipedia.org/wiki/Unmanned\\_aerial\\_vehicle](http://en.wikipedia.org/wiki/Unmanned_aerial_vehicle)

3.

[http://today.reuters.co.uk/news/articlenews.aspx?type=worldNews&storyID=2006-08-07T214710Z\\_01\\_L07879623\\_R](http://today.reuters.co.uk/news/articlenews.aspx?type=worldNews&storyID=2006-08-07T214710Z_01_L07879623_R)

[TRUKOC\\_0\\_UK-MIDEAST-ISRAEL-DRONE.xml](#)

4. <http://www.defensetech.org/archives/002369.html>

5. <http://www.armscontrol.ru/UAV/report.htm>

6.

[http://en.wikipedia.org/wiki/Unmanned\\_Combat\\_Air\\_Vehicle](http://en.wikipedia.org/wiki/Unmanned_Combat_Air_Vehicle)

497



## **Google Hacking for Cryptographic Secrets (2006-09-07 19:10)**

[1]

Interesting perspective, for sure could prove handy on a [2]nation-wide scale. The concept of [3]googling for

private keys has been around for quite a while, and here's an informative paper emphasising on how [4]Google can

Reveal Cryptographic Secrets taking the topic even further :

*" Google hacking is a term to describe the search queries that find out security and privacy flaws. Finding vulnerable servers and web applications, server fingerprinting, accessing to admin and user login pages and revealing*

*username-passwords are all possible in Google with a single click. Google can also reveal secrets of cryptography*

*applications, i.e., clear text and hashed passwords, secret and private keys, encrypted messages, signed messages*

*etc. In this paper, advanced search techniques in Google and the search queries that reveal cryptographic secrets are explained with examples in details. "*

Comments on : **Hashed passwords, Secret Keys, Public Keys, Private Keys, Encrypted Files, Signed Messages**

- external comments on [5]packed binary patterns, [6]malware functions, and the [7]malware search engine itself.

[8]Google is so not the root of the problem, although at least theoretically [9]malicious web crawling is indeed

possible. Seems like patterns come useful to both sides of the front - [10]and [11]everyone in between.

1.

[http://photos1.blogger.com/blogger/1933/1779/1600/malicious\\_crawler.0.jpg](http://photos1.blogger.com/blogger/1933/1779/1600/malicious_crawler.0.jpg)

2. <http://ddanchev.blogspot.com/2006/05/nation-wide-google-hacking-initiative.html>



3. <http://johnny.ihackstuff.com/index.php?module=prodreviews&func=showcontent&id=364>
4. [http://th.informatik.uni-mannheim.de/people/tatli/pub/ghack\\_crypto.pdf](http://th.informatik.uni-mannheim.de/people/tatli/pub/ghack_crypto.pdf)
5. <http://blogs.securiteam.com/index.php/archives/513>
6. <http://asert.arbornetworks.com/2006/07/googling-for-malware-bobbing-for-mass-mailers/>
7. <http://ddanchev.blogspot.com/2006/07/malware-search-engine.html>
8. <http://www.google.com/support/webmasters/bin/topic.py?topic=8459>
9. <http://ddanchev.blogspot.com/2006/06/malicious-web-crawling.html>
10. [http://www.boingboing.net/2006/09/06/how\\_to\\_find\\_confidence.html](http://www.boingboing.net/2006/09/06/how_to_find_confidence.html)
11. <http://www.google.com/search?hl=en&q=confidential+%22do+not+distribute%22>

498



## **Benchmarking and Optimising Malware (2006-09-08 03:43)**

[1]

With the [2]growth and diversity of today's malware, performance criteria for a malicious code is reasonably

neglected as a topic of interest, but that shouldn't be the case, as "the enemy you know is better than the enemy you don't know". As information warfare and malware often intersect for the purpose of balancing asymmetric forces, or conducting espionage, there're already research initiatives for [3]multi-platform, multi-communication-environment code.

José M. Fernandez and Pierre-Marc Bureau constructively build awareness on how "the best is yet to come" in their research on [4]Optimising Malware :

*" In this paper, we address and defend the commonly shared point of view that the worst is very much yet to*

*come. We introduce an aim-oriented performance theory for malware and malware attacks, within which we identify*

*some of the performance criteria for measuring their "goodness" with respect to some of the typical objectives for*

*which they are currently used. We also use the OODA-loop model, a well known paradigm of command and control*

*borrowed from military doctrine, as a tool for organising (and reasoning about) the behavioural characteristics*

*of malware and orchestrated attacks using it. We then identify and discuss particular areas of malware design*

*and deployment strategy in which very little development has been seen in the past, and that are likely sources of*

*increased future malware threats. Finally, we discuss how standard optimisation techniques could be applied to*

*malware design, in order to allow even moderately equipped malicious actors to quickly converge towards optimal*

*malware attack strategies and tools fine-tuned for the current Internet. "*

They've successfully distinguished the following generic and specific aim-oriented performance criteria :

### **Generic**

- Number of hosts
- Persistence
- Anonymity

### **Fraud**

- Money
- Credibility

### **Information theft**

- Penetration
- Stealth
- Amount of information
- Host location

### **Access sale**

- Upstream bandwidth
- Security

## **Destruction**

- Propagation
- Upstream bandwidth
- Host location
- Damage

## **Information Warfare**

499

- Speed
- Host Location
- Damage
- Exposure

Taking into consideration the [5]OODA loop concept – Observation, Orientation, Decision, Action – the characteristics would get definitely improved with the time.

## **Related resources and recent posts:**

[6]Malware

[7]Virus Outbreak Response Time

[8]Malware Bot Families - Technology and Trends

## [9]Malware Statistics on Social Networking Sites

1. [http://photos1.blogger.com/blogger/1933/1779/1600/Malicious\\_Pacman.0.jpg](http://photos1.blogger.com/blogger/1933/1779/1600/Malicious_Pacman.0.jpg)
2. <http://www.linuxsecurity.com/docs/malware-trends.pdf>
3. <http://www.au.af.mil/au/awc/awcgate/afri/cybercraft.pdf>
4. [http://www.scs.carleton.ca/~dsg/dss/materials/dss\\_paper\\_20060131.pdf](http://www.scs.carleton.ca/~dsg/dss/materials/dss_paper_20060131.pdf)
5. [http://en.wikipedia.org/wiki/OODA\\_Loop](http://en.wikipedia.org/wiki/OODA_Loop)
6. <http://del.icio.us/DDanchev/Malware>
7. <http://ddanchev.blogspot.com/2006/08/virus-outbreak-response-time.html>
8. <http://ddanchev.blogspot.com/2006/08/virus-outbreak-response-time.html>
9. <http://ddanchev.blogspot.com/2006/08/malware-statistics-on-social.html>

500



## **Email Spam Harvesting Statistics (2006-09-08 04:25)**

[1]Web application email harvesting has always represented an untapped threat, and it's not the basics of parsing

or web application vulnerabilities I have in mind, but the already stored, in-transit, and saved contacts by infected

people and their (insecure) platforms.

[2]Malware is already averaging 1 piece in 600 social networking pages, which isn't surprising and is greatly

proportional with the rise of [3]web application vulnerabilities. Compared to [4]personal data security breaches

capable of providing the freshest and most recent emails of the parties involved, thus resetting a spammer's activities

lifecycle, web email harvesting is still a rather common event.

Thankfully, there're already scaled initiatives such as the [5]Distributed Spam Harvester Tracking Network mak-

ing an impact :

*" Project Honey Pot is the first and only distributed system for identifying spammers and the spambots they*

*use to scrape addresses from your website. Using the Project Honey Pot system you can install addresses that are*

*custom-tagged to the time and IP address of a visitor to your site. If one of these addresses begins receiving email we not only can tell that the messages are spam, but also the exact moment when the address was harvested and the IP*

*address that gathered it.*

*To participate in Project Honey Pot, webmasters need only install the Project Honey Pot software somewhere*

*on their website. We handle the rest — automatically distributing addresses and receiving the mail they generate. As a result, we anticipate installing Project Honey Pot should not increase the traffic or load to your website. "*

### **Some current project statistics:**

- Spam Trap Addresses Monitored - **1,354,582**
- Total Spam Received - **1,464,090**
- Total Spam Servers Identified - **499,310**
- IPs Monitored - **611,368**
- Total Harvesters Identified - **10,653**

[6]Donate a MX record, or get yourself [7]an account and start contributing.

On the other hand, the host

that's web crawling for fresh emails today, will definitely match with the one found in a phishing email at a later stage

- the growing transparency and the pressure put on spammers inevitably results in the Ecosystem I mentioned in my

[8]Malware - Future Trends research.

### **Related posts:**

[9]The Beauty of the Surrealistic Spam Art

[10]Real-Time PC Zombie Statistics

[11]The current state of IP spoofing

[12]Dealing with Spam - The O'Reilly.com Way

1. <http://ddanchev.blogspot.com/2006/06/web-application-email-harvesting-worm.html>

2. <http://ddanchev.blogspot.com/2006/08/malware-statistics-on-social.html>

3. <http://ddanchev.blogspot.com/2006/05/current-state-of-web-application-worms.html>

4. <http://ddanchev.blogspot.com/2006/01/personal-data-security-breaches.html>

5. <http://www.projecthoneypot.org/>

6. <http://www.projecthoneypot.org/faq.php#d>

7. [http://www.projecthoneypot.org/create\\_account.php](http://www.projecthoneypot.org/create_account.php)

8. <http://www.linuxsecurity.com/docs/malware-trends.pdf>

501

9. <http://ddanchev.blogspot.com/2006/07/beauty-of-surrealistic-spam-art.html>

10. <http://ddanchev.blogspot.com/2006/06/real-time-pc-zombie-statistics.html>

11. <http://ddanchev.blogspot.com/2006/02/current-state-of-ip-spoofing.html>

12. <http://ddanchev.blogspot.com/2006/06/dealing-with-spam-oreillycom-way.html>





## **A Study on The Value of Mobile Location Privacy (2006-09-08 16:18)**

[1]

Right in between [2]Flickr's introduction of geotagging, the term stalkerazzi got its necessary attention, then

again it entirely depends on you to evolve as a Web 2.0 user and add more value to the ongoing folksonomy, or

realize the possible privacy implications.

Yesterday, Danezis Cvrcek and Matyas Kumpost released an interesting [3]study on The Value of Location Pri-

vacy :

*" This paper introduces results of a study into the value of location privacy for individuals using mobile devices.*

*We questioned a **sample of over 1200 people from five EU countries, and used tools from experimental psychology***

***and economics to extract from them the value they attach to their location data.** We compare this value across national groups, gender and technical awareness, but also the perceived difference between academic use and*

*commercial exploitation. We provide some analysis of the self-selection bias of such a study, and look further at the*

*valuation of location data over time using data from another experiment. "*

[4]While there're indeed [5]privacy issues related to mobile devices, in the age of malware authors purchasing

commercial IP Geolocation services to get a better grasp of the infected sample, and [6]Google's growing concern on

the use of networks such as Tor mimicking possible malicious behavior you should ask yourself, what is it that you're

trying to achieve, [7]Anonymity or Privacy preservation online and go for it without feeling like a hostage.

1.

<http://photos1.blogger.com/blogger/1933/1779/1600/naked-surfer-01.jpg>

2. [http://blog.wired.com/monkeybites/index.blog?entry\\_id=1546974](http://blog.wired.com/monkeybites/index.blog?entry_id=1546974)

3.

[http://www.buslab.org/index.php/component?option=com\\_repository/Itemid,33/func,fileinfo/id,163/parent,cat](http://www.buslab.org/index.php/component?option=com_repository/Itemid,33/func,fileinfo/id,163/parent,category/)

[egory/](http://www.buslab.org/index.php/component?option=com_repository/Itemid,33/func,fileinfo/id,163/parent,category/)

4. <http://www.geekzone.co.nz/content.asp?contentid=6628>

5. <http://ddanchev.blogspot.com/2006/03/privacy-issues-related-to-mobile-and.html>

6.

[http://www.boingboing.net/2006/09/07/google\\_blocking\\_priv.html](http://www.boingboing.net/2006/09/07/google_blocking_priv.html)

7. <http://ddanchev.blogspot.com/2006/01/anonymity-or-privacy-on-internet.html>

503



## **The Freedom Tower - 11th September 2006 (2006-09-11 20:57)**

[1]

That's of course [2]how it's gonna look like in 2012 - true leaders never look into the past, they're too

busy defining the future. Time goes fast given you're busy and always up to something - disruption! I still clearly

remember the moment when 9/11 happened and realize how much I've changed since then. Mixed thoughts started

buzzing around my mind, the type of thoughts

[3]Cryptome's Daily Photos smartly emphasises on. Anyway, someone

or something always has to, either be the result, the consequence, or the foundation for the next stage. I'll leave it

open to interpretations on what interacts with what :

Cold War <=> **Defense/Intelligence**  
**spending/Innovation** <=> Post 9/11 World

Terrorist <=> **Ideology** <=> War

Foreign policy <=> Terrorism <=> **Geopolitical**  
**dominance**

Terrorism <=> **OSINT** <=> Intelligence

Civil Liberties <=> **Terrorism** <=> Surveillance

Poverty <=> **G8** <=> Developed world

Space exploration budget cuts <=> **Terrorism** <=>  
Alternative energy sources development

**Paranoia** <=> Terrorism <=> Security services/products  
market growth

I can keep on going, but that's not the point, the point is  
how globalisation is acting as a double edged sword,

and so is paranoia, still, keep in mind that there're [4]one  
million other ways to get killed compared to a terrorist

attack.

There've always been and will always be "bad guys", "good  
guys", and "greyhat guys" - barking dogs of course -

trouble is knowing whom to trust at a particular moment in  
time. I can easily argue that during the past five years,

all the "bad guys" had to do was to go through the press  
and come up "future long term strategies" perceptual  
enough to shock and awe "the infidels". My point is that,  
OSINT is also a double edged sword, useful and dangerous  
to both parties. As far as the infidels are concerned, I'm not  
one - I believe in myself!

**Underestimating an adversary is much worse than  
overestimating it**, just cut using terrorism as the excuse

for everything you do, or are about to do, which is as  
subjective as China's economy taking over the world -

something neither the "bad guys" nor China would do.

### **Related posts:**

[5]Terrorism

[6]Data mining, terrorism and security

[7]Terrorist Social Network Analysis

[8]Benefits of Open Source Intelligence - OSINT

[9]Visualization, Intelligence and the Starlight project

[10]Cyber terrorism - don't stereotype and it's there!

[11]Cyber terrorism - recent developments

[12]Arabic Extremist Group Forum Messages' Characteristics

[13]Tracking Down Internet Terrorist Propaganda

[14]Cyber Terrorism Communications and Propaganda

[15]Steganography and Cyber Terrorism Communications

1.  
<http://photos1.blogger.com/blogger/1933/1779/1600/Freedom.jpg>

2. <http://blog.wired.com/freedomtower/>

3. <http://cryptome.org/cdphotos.htm>

4. <http://www.wired.com/news/technology/0,71743-0.html>

5. <http://del.icio.us/DDanchev/Terrorism>

6. <http://ddanchev.blogspot.com/2006/03/data-mining-terrorism-and-security.html>
7. <http://ddanchev.blogspot.com/2006/05/terrorist-social-network-analysis.html>
8. <http://ddanchev.blogspot.com/2006/09/benefits-of-open-source-intelligence.html>
9. <http://ddanchev.blogspot.com/2006/01/visualization-intelligence-and.html>
10. <http://ddanchev.blogspot.com/2005/12/cyberterrorism-dont-stereotype-and-its.html>
11. <http://ddanchev.blogspot.com/2006/01/cyberterrorism-recent-developments.html>
12. <http://ddanchev.blogspot.com/2006/05/arabic-extremist-group-forum-messages.html>
13. <http://ddanchev.blogspot.com/2006/06/tracking-down-internet-terrorist.html>
14. [http://ddanchev.blogspot.com/2006/08/cyber-terrorism-communications-and\\_22.html](http://ddanchev.blogspot.com/2006/08/cyber-terrorism-communications-and_22.html)
15. <http://ddanchev.blogspot.com/2006/08/steganography-and-cyber-terrorism.html>

505



**NSA's Terrorist Records Database (2006-09-11 20:59)**

[1]

Right on time! Inside sources – this is a creative spoof – at the NSA finally coordinated their intelligence sharing

efforts with the [2]Patriot Search, and came up with a public [3]database giving you the opportunity to lookup your entire neighborhood for suspicious relations with the Middle East.

What's the bottom line? [4]Keep your friends close, your intelligence buddies closer!

Interested in [5]Anti-Terror tips? Follow these :

- Use email software with strong encryption to prevent terrorists from reading your email
- Encrypt the files on your computer using strong encryption such as PGP to prevent terrorists from accessing your files
- Browse the web using an anonymous proxy to prevent terrorists from seeing what sites you visit
- Insist that electronic voting machines provide you with a traceable paper receipt so you can ensure that terrorists haven't altered the electronic ballot
- Report all behavior, especially if it is suspicious

1. [http://photos1.blogger.com/blogger/1933/1779/1600/terrorist\\_database\\_hoax.jpg](http://photos1.blogger.com/blogger/1933/1779/1600/terrorist_database_hoax.jpg)

2. <http://blog.outer-court.com/patriot/>

3. <http://www.nsatt.org/>

4. <http://ddanchev.blogspot.com/2006/01/keep-your-friends-close-your.html>

5. <http://www.nsatt.org/tips.php>

506



## **Secret CIA Prisons (2006-09-11 21:02)**

[1]

It's official, [2]there're indeed (publicly) secret CIA prisons, and a public commitment towards improvement :

*" All suspects will now be treated under new guidelines issued by the Pentagon on Wednesday, which bring all military detainees under the protection of the Geneva Convention. The move marks a reversal in policy for the Pentagon, which previously argued that many detainees were unlawful combatants who did not qualify for such protections. The new guidelines forbid all torture, the use of dogs to intimidate prisoners, water boarding - the practice of submerging prisoners in water - any kind of sexual humiliation, and many other interrogation techniques. "*

I assume operating such facilities in the Twilight Zone is flexible from an interrogation point of view, what



makes me wonder though is how [3]justified kidnappings of alleged terrorists by recruiting local intelligence agents

are. Guess a guy I had a hot discussion with the other night was right, no more Russian skirmishes in guerilla warfare,

the adversary leaders just dissapear and no one, even their forces ever hear anything of them – spooky special forces

stealing the hive's queen.

In case you're also interested in [4]DoD's New Detainee Interrogation Policy, it's already available at the FAS's

blog, plus [5]"biographies" of 14 detainees.

However, there's one thing the entire [6]synthetic community would always be thankful to the CIA though,

and that's [7]the LSD, a proven "[8]ice breaker" during the decades.

Graph courtesy of Spiegel.de

1.

[http://photos1.blogger.com/blogger/1933/1779/1600/United\\_Intelligence\\_Airlines.jpg](http://photos1.blogger.com/blogger/1933/1779/1600/United_Intelligence_Airlines.jpg)

2. <http://news.bbc.co.uk/2/hi/americas/5321606.stm>

3. [http://news.xinhuanet.com/english/2006-07/05/content\\_4798820.htm](http://news.xinhuanet.com/english/2006-07/05/content_4798820.htm)

4.

[http://www.fas.org/blog/secretcy/2006/09/dod\\_unveils\\_detainee\\_interroga.html](http://www.fas.org/blog/secretcy/2006/09/dod_unveils_detainee_interroga.html)

5. <http://www.fas.org/irp/news/2006/09/detaineebios.pdf>

6. <http://www.erowid.org/>

7. <http://www.mindcontrolforums.com/lsd-mc-cia.htm>

507

8.

[http://www.totse.com/en/politics/central\\_intelligence\\_agency/ciacid.html](http://www.totse.com/en/politics/central_intelligence_agency/ciacid.html)

508



## **Visualizing Enron's Email Communications (2006-09-12 05:33)**

[1]

In a previous post "[2]There You Go With Your Financial Performance Transparency" I mentioned the release

of [3]Enron's email communications between 2000/2002, mind you, by Enron's ex-risk management provider.

Continuing the series of resourceful posts on [4]visualizing terrorists, [5]intelligence data sharing, [6]security and

new media, here's Jeffrey Heer's [7]visual data mining of Enron's email communications sample :

*" Using the Enron e-mail archive as a motivating dataset, we are attempting the marriage of visual and algo-*

*rithmic analyses of e-mail archives within an exploratory data analysis environment. The intent is to leverage the*

*characteristic strengths of both man and machine for unearthing insight. Below are a few sketches from a preliminary exploration into the design space of such tools.*  
"

And here's how he [8]visualized the social network, invaluable "big picture".

1.

[http://photos1.blogger.com/blogger/1933/1779/1600/med\\_search3\\_california\\_ferc.png](http://photos1.blogger.com/blogger/1933/1779/1600/med_search3_california_ferc.png)

2. <http://ddanchev.blogspot.com/2006/06/there-you-go-with-your-financial.html>

3. <http://www.enronemail.com/>

4. <http://ddanchev.blogspot.com/2006/05/terrorist-social-network-analysis.html>

5. <http://ddanchev.blogspot.com/2006/01/visualization-intelligence-and.html>

6. <http://ddanchev.blogspot.com/2006/03/visualization-in-security-and-new.html>

7. <http://jheer.org/enron/>

8. <http://jheer.org/enron/v1/>

509



**Google Anti-Phishing Black and White Lists (2006-09-13 02:08)**

[1]

Can the world's most effective search engine manage to keep [2]questionable sites away from the search

results of its users? Seems like its toolbar users are also [3]warned about such. Google for sure got the widest and most recent snapshot of the Web to draw up conclusions from, and seems like starting from the basics of keeping

a black and white list with questionable sites/URLs is still taken into consideration. Googling Google proves handy

sometimes and you can stumble upon interesting findings such as Google's [4]Black - [5]cache version - and [6]White

lists of phishing and possible fraudulent sites - there's still a [7]cached version of the White list available and the

[8]white domains as well.

As I often say that the [9]host trying to 6667 its way out of the network today, will be the one sending

phishing and spam mails tomorrow, therefore in order to verify I took a random blacklisted host such as

[10]<http://219.255.134.12/fdic.gov/index.html.html> and decided to first test it at [11]TrustedSource, and of

course, at the [12]SORBS to logically figure out that the host's has been indeed :

*" Spam Sending Trojan or Proxy attempted to send mail from/to from= to="*

What's ruining the effect of black and white lists? With today's [13]modular malware - and [14]DIY phishing

toolkits – the list of IP’s currently hosting phishing sites can become a decent time-consuming effort to keep track

of, namely black lists can be sometimes rendered useless given how malware-infected hosts increasingly act as

spamming, phishing, and botnet participating ones – if ISPs were given the incentives or obliged to take common

sense approaches for dealing with malware infected hosts, it would make a difference. As far as the white lists are

concerned, [15]XSS vulnerabilities on the majority of top domains, and browser specific vulnerabilities make their

impact, but most of all, it’s a far more complex issue than black and white only.

Another recent and free initiative I came across to, is the [16]Real-Time Phishing Sites Monitor, which may

prove useful to everyone interested in syndicating their findings.

[17]Third-party anti-phishing toolbars, as well as anti-phishing features build within popular toolbars are not

the panacea of dealing with phishing attacks. A combination of them and user awareness, thus less gullible user is

the way.

1. <http://photos1.blogger.com/blogger/1933/1779/1600/scam.jpg>

2. <http://www.stopbadware.org/>

3.

<http://img217.imageshack.us/img217/7352/googlefraudwh7.png>

4. <http://sb.google.com/safebrowsing/update?version=goog-black-url:1:-1>

5. <http://64.233.161.104/search?q=cache:kLfqnC7pgYJ:sb.google.com/safebrowsing/update%3Fversion%3Dgoog-black>

[-url:1:-1+site:sb.google.com+paypal.com&hl=en&ct=clnk&](http://64.233.161.104/search?q=cache:kLfqnC7pgYJ:sb.google.com/safebrowsing/update%3Fversion%3Dgoog-black-url:1:-1+site:sb.google.com+paypal.com&hl=en&ct=clnk&)

6. <http://sb.google.com/safebrowsing/update?version=goog-white-url:1:-1>

7. [http://64.233.161.104/search?q=cache:RoFxYPy\\_jTEJ:sb.google.com/safebrowsing/update%3Fversion%3Dgoog-white](http://64.233.161.104/search?q=cache:RoFxYPy_jTEJ:sb.google.com/safebrowsing/update%3Fversion%3Dgoog-white)

[=url:1:-1+site:sb.google.com+paypal.com&hl=en&ct=c](http://64.233.161.104/search?q=cache:RoFxYPy_jTEJ:sb.google.com/safebrowsing/update%3Fversion%3Dgoog-white-url:1:-1+site:sb.google.com+paypal.com&hl=en&ct=c)

8. <http://sb.google.com/safebrowsing/update?version=goog-white-domain:1:-1>

9. <http://ddanchev.blogspot.com/2006/02/master-of-infected-puppets.html>

10. <http://219.255.134.12/fdic.gov/index.html.html>

11. <http://www.trustedsource.org/>

12. <http://www.us.sorbs.net/lookup.shtml>

13. <http://www.linuxsecurity.com/docs/malware-trends.pdf>

14.

[http://www.sophos.com/pressoffice/news/articles/2004/08/sa\\_diy.phishing.html](http://www.sophos.com/pressoffice/news/articles/2004/08/sa_diy.phishing.html)

15. [http://web3.m34s11.vlinux.de/xss\\_research.htm](http://web3.m34s11.vlinux.de/xss_research.htm)

16. <http://phishery.internetdefence.net/rtmonitor.cgi>

510

17. <http://ddanchev.blogspot.com/2006/03/anti-phishing-toolbars-can-you-trust.html>

511



## **Testing Intrusion Prevention Systems (2006-09-13 22:00)**

[1]

Informative testings results of various [2]IPSs such as [3]Juniper IDP 200, [4]Cisco IPS 4240, [5]eSoft ThreatWall 200, [6]ForeScout ActiveScout 100, [7]McAfee IntruShield 2700.

Here's how they tested :

*" In order to create a base environment in which to compare the different appliances, we set up a single sys-*

*tem within our test network to be the target of Core Impact's simulated attacks. We chose a system running the*

*most vulnerable operating system we could think of— Windows 2000 Service Pack 2 with no additional service*

*packs or security updates. We temporarily opened the channels on the test network's firewall and installed Core*

*Impact on a system outside the network. We then proceeded to detect and "attack" the Windows 2000 system to identify its vulnerabilities. Of the hundreds of attack modules available, we picked 85 of the most applicable.*

*Knowing how our target system was vulnerable and the attacks we could launch against it, we connected each IPS*

*in turn according to its recommended configuration. We then allowed each IPS to function in a real-world network*

*environment for a day or more. Eventually we rebooted the Windows 2000 machine and ran Core Impact to simulate*

*a barrage of intrusions. Finally, we adjusted the security profiles of each IPS and ran the tests one more time.*

*The result was a complete picture of how effective each IPS was at preventing attacks—both out of the box and*

*after fine-tuning. The good news is, we were able to tweak each IPS to completely shut down the Core Impact attacks. "*

There are, however, hidden costs related to IPSs, and that's increased maintainance and reconfiguration time,

possible decline in productivity. The key is understanding the pros and cons of your solution, educating the masses

of users, and run a departamental, compared to a comany-wide enforcement at the first place as far as host based

IPS are concerned. Network based IPSs sensitivity is proportional to the level of false alerts generated, so figure



out

how to balance and adapt the solution to your network.

Suspicious system behaviour is such an open topic term to the majority of end users, keep it in mind whatever you

do when dealing with HIPS. And do [8]your [9]homework of course.

1. [http://www.gcn.com/print/25\\_27/41911-1.html](http://www.gcn.com/print/25_27/41911-1.html)
2. [http://en.wikipedia.org/wiki/Intrusion\\_prevention\\_system](http://en.wikipedia.org/wiki/Intrusion_prevention_system)
3. [http://www.gcn.com/print/25\\_27/41906-1.html](http://www.gcn.com/print/25_27/41906-1.html)
4. [http://www.gcn.com/print/25\\_27/41908-1.html](http://www.gcn.com/print/25_27/41908-1.html)
5. [http://www.gcn.com/print/25\\_27/41912-1.html](http://www.gcn.com/print/25_27/41912-1.html)
6. [http://www.gcn.com/print/25\\_27/41913-1.html](http://www.gcn.com/print/25_27/41913-1.html)
7. [http://www.gcn.com/print/25\\_27/41905-1.html](http://www.gcn.com/print/25_27/41905-1.html)
8. <http://www.securityfocus.com/infocus/1670>
9. <http://www.scmagazine.com/us/suppliers/listing/89283/intrusion-prevention-systems/>

512



## **Vulnerabilities in Emergency SMS Broadcasting (2006-09-13 22:07)**

[1]

There's been a recent [2]test of emergency cell phone alert in the Netherlands – original article was [3]here

– and while broadcasting supposedly reaches the largest number of people in the surrounding area, timing and countless number of factors also matter :

*" Cell phones throughout a downtown hotel beeped simultaneous Tuesday with an alert: there is a suspicious*

*package in the building. It was a drill, run by Dutch authorities testing an emergency "cell broadcasting" system that sends a text message to every mobile phone in a defined area. Representatives from 21 national governments, New*

*York City and the U.S. Federal Emergency Management Agency, or FEMA, watched the signal go out to cell phones*

*throughout the Sofitel hotel in Amsterdam. About half the people in the building then followed instructions and*

*evacuated. "We want to see what worked and what didn't," said David Webb, of FEMA's Urban Search and Rescue Program. "The EU (European Union) is really leading the way with this technology. "*

### **What if :**

- Even in case that key emergency personnel were to use a separate communication network, radio for instance,

broadcasting to anyone accepting could result in significant delays, and even though the message is sent, it doesn't

mean it would take advantage of the momentum

- [4]cell phone jammers are often used by hotels to preserve the unique atmosphere and undisturbed confer-

ence meetings can prove contradictory, excluding the fact that the parties supposedly plotting the attack don't use

one by themselves

- despite the fact that [5]one in five will pick up their mobile during sex, how many obsessively check for newly arrived sms messages?

- how would a tourist know how to successfully authenticate the local authorities at the first place, in case of

emergencies watch out for an sms from 010101, now I assume you know how easily I can sms you from the same

number and impersonate the number

- what should the user be mostly aware of be aware of, mobile malware, SMSishing, or "call this 0 900 or else

I won't tell you where's the attack" type of messages

- from a multilingual point of view, will it be using English by default, and how many would be still enjoying

their meals while everyone's leaving

Great idea, but it may prove challenging to evaluate the actual results in a timely manner. Sent doesn't mean

received or read on time, even actioned upon.

### **Recommended reading:**

[6]SMS disaster alert and warning systems - don't do it !

[7]Revisiting SMS during Disasters

[8]Concept Paper on Emergency Communications during Natural Disasters

[9]Exploiting Open Functionality in SMS- Capable Cellular Networks

[10]The Role of Mobiles in Disasters and Emergencies

1.

<http://photos1.blogger.com/blogger/1933/1779/1600/alerts.gif>

2. <http://cms.firehouse.com/content/article/article.jsp?sectionId=46&id=51061>

3. <http://64.233.161.104/search?q=cache:Llels3m46TMJ:www.chron.com/disp/story.mpl/ap/fn/4164397.html+Dutch+Te>

[513](#)

[st+Emergency+Cell+Phone+alert&hl=en&ct=clnk&cd=1](#)

4. <http://www.spyzone.com/ProductDetails.aspx?productID=544&selection=7&category=26>

5.

[http://money.cnn.com/2006/08/25/technology/fastforward\\_kirkpatrick.fortune/index.htm?section=money\\_technolo](http://money.cnn.com/2006/08/25/technology/fastforward_kirkpatrick.fortune/index.htm?section=money_technolo)

[gy](#)

6.

[http://www.spy.org.uk/spyblog/2005/01/sms\\_disaster\\_alert\\_and\\_warning.html](http://www.spy.org.uk/spyblog/2005/01/sms_disaster_alert_and_warning.html)

7. <http://www.knowprose.com/node/10312>

8.

[http://tsunami.ait.ac.th/Documents/disaster\\_communication\\_assistance\\_concept\\_paper.pdf](http://tsunami.ait.ac.th/Documents/disaster_communication_assistance_concept_paper.pdf)

9. <http://www.patrickmcdaniel.org/talks/sms-briefing-10-05.pdf>

10.

<http://www.enlightenmenteconomics.com/disasterreport.pdf>

514



## **Malware on Diebold Voting Machines (2006-09-13 22:50)**

[1]

Continuing the previous post on "[2]How to Win the U.S Elections" seems like malware is indeed [3]diebold

voting machines compatible - [4]related videos.

The main [5]findings of the study are:

*- Malicious software running on a single voting machine can steal votes with little if any risk of detection. The*

*malicious software can modify all of the records, audit logs, and counters kept by the voting machine, so that even*

*careful forensic examination of these records will find nothing amiss. We have constructed demonstration software*

*that carries out this vote-stealing attack.*

*- Anyone who has physical access to a voting machine, or to a memory card that will later be inserted into a*

*machine, can install said malicious software using a simple method that takes as little as one minute. In practice, poll workers and others often have unsupervised access to the machines.*

*- AccuVote-TS machines are susceptible to voting-machine viruses — computer viruses that can spread mali-*

*cious software automatically and invisibly from machine to machine during normal pre- and post-election activity.*

*We have constructed a demonstration virus that spreads in this way, installing our demonstration vote-stealing*

*program on every machine it infects.*

*- While some of these problems can be eliminated by improving Diebold's software, others cannot be remedied*

*without replacing the machines' hardware. Changes to election procedures would also be required to ensure security.*

IP enabled, Windows running ATM's with anti-virus, IPv6 enabled fridges with anti-virus, smart phones with

anti-virus, Play Stations with anti-virus, birds as early warning systems for an epidemic, so where's my signature,

dude?

1.

<http://photos1.blogger.com/blogger/1933/1779/1600/hallow>

[een.gif](#)

2. <http://ddanchev.blogspot.com/2006/07/how-to-win-us-elections.html>

3. <http://itpolicy.princeton.edu/voting/>

4. <http://itpolicy.princeton.edu/voting/videos.html>

5. <http://itpolicy.princeton.edu/voting/summary.html>

515



## **Prosecuting Defectors and Appointing Insiders (2006-09-13 23:14)**

[1]

In the year 2006, those who control Russia's energy reserves control a huge portion of the world's energy

market - [2]renewable energy is the future. And as you can imagine they're for sure not controlled by some newly

born [3]Russian millionaires - a great benchmark for how vibrant a country's economy or level of corruption really is.

Seems like the long-term effects of a [4]planned economy are still a political doctrine, and the invisible hand of the

market is still short enough to feel the Russian energy sector as [5]Russian intelligence chief's son has been named

adviser to oil company chairman :

*" A son of the head of Russia's main intelligence agency has been named an adviser to the chairman of state*

*oil company OAO Rosneft, the daily newspaper Kommersant reported Wednesday, citing an unidentified source on*

*Rosneft's board of directors. Andrei Patrushev, the 25-year-old son of Federal Security Service (FSB) director Nikolai Patrushev, had previously been an FSB official himself, working in the department that keeps tabs on the Russian oil industry, according to Kommersant. "*

The courage to rise above shown by [6]Mikhail Khodorkovsky has its own butterfly effect, and it's so easily

predictable one. Here's a [7]Google bomb for you – it means enemy of the people. Here's [8]another. [9]Bpar

народа or a vivid [10]protectionist?

1.

<http://photos1.blogger.com/blogger/1933/1779/1600/spy.jpg>

2. [http://en.wikipedia.org/wiki/Renewable\\_energy](http://en.wikipedia.org/wiki/Renewable_energy)

3. <http://www.cdi.org/russia/johnson/9174-9.cfm>

4. [http://en.wikipedia.org/wiki/Planned\\_economy](http://en.wikipedia.org/wiki/Planned_economy)

5.

[http://www.iht.com/articles/ap/2006/09/13/business/EU\\_FIN\\_COM\\_Russia\\_Rosneft.php](http://www.iht.com/articles/ap/2006/09/13/business/EU_FIN_COM_Russia_Rosneft.php)

6. [http://en.wikipedia.org/wiki/Mikhail\\_Khodorkovsky](http://en.wikipedia.org/wiki/Mikhail_Khodorkovsky)

7. [http://www.google.com/search?](http://www.google.com/search?hl=en&lr=&q=%D0%B2%D1%80%D0%B0%D0%B3+%D0%)

[hl=en&lr=&q=%D0%B2%D1%80%D0%B0%D0%B3+%D0%](http://www.google.com/search?hl=en&lr=&q=%D0%B2%D1%80%D0%B0%D0%B3+%D0%)



[BD%D0%B0%D1%80%D0%BE%D0%B4%D0%B0](#)

8. <http://www.google.com/search?hl=en&lr=&q=miserable+failure>

9. [http://ru.wikipedia.org/wiki/%C3%90%C2%92%C3%91%C2%80%C3%90%C2%B0%C3%90%C2%B3\\_%C3%90%C2%BD%C3%90%C2%B0%C3%9](http://ru.wikipedia.org/wiki/%C3%90%C2%92%C3%91%C2%80%C3%90%C2%B0%C3%90%C2%B3_%C3%90%C2%BD%C3%90%C2%B0%C3%9)

[1%C2%80%C3%90%C2%BE%C3%90%C2%B4%C3%90%C2%B0](#)

10. <http://en.wikipedia.org/wiki/Protectionism>

516



## **Internet PSYOPS - Psychological Operations (2006-09-14 13:11)**

[1]

Psychological operations or [2]PSYOPS is an indirect use of [3]information warfare methods to deceive,

shape and influence the behavior and attitude of the targeted audience – military marketers with greater access to

resources and know-how. The Internet acting as a global-reaching, cost-effective platform for dissemination of a

message, rumor, lie, inside information is directly influencing the evolution of the concept.

You may find this research conducted back in 2001, still relevant on the basics of psychological operations and

propaganda online. A brief summary of [4]The Internet and Psychological Operations :

*" As an information medium and vehicle of influence, the Internet is a powerful tool, in both open societies as well as in those whose only glimpse of the outside world is increasingly viewed and shaped through webpages,*

*E-mail, and electronic chat rooms. Moreover, the sword cuts both ways, as unconstrained (legally, socially, politically) adversaries find the Internet an effective vehicle for influencing popular support for their cause or inciting the*

*opposite against the U.S. or its interests. Consequently, the realm of military psychological operations (PSYOP) must be expanded to include the Internet. Just as obvious is the need for action to remove or update current policy and*

*legal constraints on the use of the Internet by military PSYOP forces, allowing them to embrace the full range of media, so that the U.S. will not be placed at a disadvantage. Although current international law restricts many aspects of*

*PSYOP either through ambiguity or noncurrency, there is ample legal room for both the U.S. and others to conduct*

*PSYOP using modern technology and media such as the Internet. Existing policy and legal restrictions, however, must*

*be changed, allowing military PSYOP forces to both defend and counter adversarial disinformation and propaganda*

*attacks which impact on the achievement of military objectives. By examining this issue, I hope to highlight the importance of the Internet for PSYOP and foment further discussion. "*

Undoubtedly, [5]Abu Ghraib's fiasco is among the most relevant cases of unintentional PSYOPS in reverse, where the

leak's echo effect would continue to spell skepticism towards what democracy really is. And while there're indeed

legal issues to consider when using such operations, what is legal and illegal in times of war is questionable.

### **Some basic examples:**

- your [6]web sites spread messages of your enemies
- [7]sms messages and your voice mail say you're about to lose the war
- your fancy military email account is inaccessible due to [8]info-warriors utilizing the power of the masses, thus script kiddies to distract the attention
- you [9]gain participation, thus support
- you feel like Johnny Mnemonic taking the elevator to pick up the 320 GB of R &D data when a [10]guerilla info-warrior appears on the screen and wakes you up on your current stage of brainwashing
- starting from the basics that the only way to [11]ruin a socialist type of government is to introduce its citizens to the joys of capitalism - it always works

- [12]hacktivism - traffic acquisition plus undermining confidence
- propaganda - [13]North Korea is quite experienced
- self-serving news items, commissioned ones
- achieving Internet echo as a primary objective
- introducing biased exclusiveness
- stating primary objectives as facts that have already happened
- impersonation

The evolution of online PSYOPS is on its way and is actively utilized by both adversaries, and everyone in be-

tween, it's entirely up to you to be either objective, or painfully subjective.

1. [http://en.wikipedia.org/wiki/Psychological\\_operations](http://en.wikipedia.org/wiki/Psychological_operations)

517

2. [http://en.wikipedia.org/wiki/Psychological\\_warfare](http://en.wikipedia.org/wiki/Psychological_warfare)

3. [http://photos1.blogger.com/blogger/1933/1779/1600/information\\_warfare.1.gif](http://photos1.blogger.com/blogger/1933/1779/1600/information_warfare.1.gif)

4. <http://ics.leeds.ac.uk/papers/pmt/exhibits/632/internetandpsyops.pdf>

5. <http://yro.slashdot.org/article.pl?sid=04/11/07/1442217>

6. <http://www.nato.int/docu/review/2001/0104-04.htm>
7. [http://www.boingboing.net/2006/07/28/israel\\_using\\_sms\\_rec.html](http://www.boingboing.net/2006/07/28/israel_using_sms_rec.html)
8. <http://ddanchev.blogspot.com/2006/09/chinese-hackers-attacking-us.html>
9. [http://www.boingboing.net/2006/07/18/image\\_of\\_the\\_day\\_chi.html](http://www.boingboing.net/2006/07/18/image_of_the_day_chi.html)
10. <http://www.theage.com.au/news/technology/israel-hacks-into-hezbollah-tv-radio/2006/08/02/1154198175078.html>
11. <http://cryptome.org/invent-intel.htm>
12. <http://ddanchev.blogspot.com/2006/02/hacktivism-tensions.html>
13. <http://ddanchev.blogspot.com/2006/08/north-koreas-strategic-developments.html>

518



### **Leaked Unmanned Aerial Vehicle Photo of Taliban Militants (2006-09-18 16:03)**

[1]

Missed shot from a predator drone due to moral concerns, remarkable move and one visionary enough not

to provoke another media fiasco of killed civilians for the sake of killing alleged militants. "[2]U.S. Military Investigates Leaked Photo"

*" The grainy black and white photo shows what NBC says are some 190 Taliban militants standing in several*

*rows near a vehicle in an open area of land. Gunsight-like brackets were positioned over the group in the photo. NBC*

*quoted one Army officer who was involved with the spy mission as saying "we were so excited" that the group had been spotted and was in the sights of a U.S. drone. But the network quoted the officer, who was not identified, as*

*saying that frustration soon set in after the officers realized they couldn't bomb the funeral under the military's rules of engagement. "*

[3]Hezbollah are also known to be able of operating drones, as well as their "window-shopping" [4]purchasing

capabilities for night vision gear but how come? Politically independent parties whose revenues get generated by

their ability to be totally neutral and, of course, tactics for bypassing gear embargoes.

However, it would be naive to assume everyone is as rational as you are, as it's a rather common practice for

various military forces to build up their foundations near highly populated areas, schools and hospitals. Insider

leaks like these show certain weaknesses, namely operatives with access to information whose significance slightly

devaluated, so why not generate some buzz on the findings.

Naturally, the [5]Pentagon is taking measures to limit the potential of yet another media fiasco, taking into

consideration the growing use of gadgets in the military. Moreover, successfully [6]realizing the power of OSINT, an

information security/web site alert was issued during August on [7]what can't be posted at .mil sites.

Predator UAV image of Serbian fighters surrendering in Kosovo, courtesy of [8]Military Intelligence Satellites.

1. [http://photos1.blogger.com/blogger/1933/1779/1600/surrender\\_predator.jpg](http://photos1.blogger.com/blogger/1933/1779/1600/surrender_predator.jpg)
2. <http://www.military.com/NewsContent/0,13319,113440,00.html>
3. <http://ddanchev.blogspot.com/2006/09/hezbollahs-use-of-unmanned-aerial.html>
4. <http://www.sfgate.com/cgi-bin/article.cgi?file=/c/a/2006/08/20/MNGK9KLVH41.DTL>
5. <http://news.bbc.co.uk/1/hi/technology/5226254.stm>
6. <http://ddanchev.blogspot.com/2006/09/benefits-of-open-source-intelligence.html>
7. <http://www.defensetech.org/archives/002695.html>
8. [http://rst.gsfc.nasa.gov/Intro/Part2\\_26e.html](http://rst.gsfc.nasa.gov/Intro/Part2_26e.html)

519

x

## **Cyber Intelligence - CYBERINT (2006-09-18 21:16)**

[1]

HUMINT, [2]SIGINT, [3]TECHINT, all concepts for gathering intelligence and supporting decision makers on



emerging trends are invaluable by their own definitions, yet useless if not coordinated for achieving the ultimate

objective. Cyberspace is so much more than a social phenomenon or the playground of countless pseudo personali-

ties. Info-warriors and analysts are realizing that Cyberspace is becoming so disperse and versatile, that a seperate

practice of Cyber Intelligence is necessary to proactively respond – and always be a step ahead of developing new

capabilities – of [4]emerging players, [5]threats, and [6]tactics. Virtual situational awareness is as important to

intelligence analysts, as it is important to security professionals wanting to remain competitive.

What's Cyber Intelligence, or Intelligence analysis for Internet security, can we model it, how long would the

model survive before what used to static turns into a sneaky variable knowing its practices has been exposed?

What would the ultimate goal of CYBERINT be? To map the bad neighborhoods and keep an eye on them, to profile

the think-tanks and assess their capabilities, background motivations for possible recruitment? Or to [7]secure

Cyberspace, no matter how megalomaniac it may sound, or to basically acquire know-how to be used in future real-life

or cyber conflicts?

[8]Intelligence Analysis for Internet Security proposes an intelligence model for the development of an overall

systems security model, here's an excerpt :

*" Obtaining prior knowledge of both threats and vulnerabilities - as well as sensitivity to possible opportunities to exploit the vulnerabilities - is essential. Intelligence analysis, of course, operates at different levels, ranging from the specific to the general, and from short-term incidents and operations to long term patterns and challenges. Each form or level of analysis is crucial, and complements and supplements the others. Nevertheless, it is important to*

*distinguish them from one another and to be clear at which level the activities are taking place. It is also important to recognize that the most critical insights will be obtained from fusion efforts that combine these different levels.*

*The several complementary levels of intelligence analysis are strategic analysis, tactical analysis and operational*

*analysis. In practice, these categories shade into each other and are not always sharply differentiated, and differing definitions for these terms exist in the intelligence community. Nevertheless, they offer a useful framework within*

*which intelligence tasks and requirements can initially be delineated. "*

A very informative and relevant research emphasizing on **strategic intelligence analysis, tactical intelligence analysis, operational intelligence analysis**, and how cyber intelligence intersects with traditional approaches.

**What's the core of CYBERINT?**

- the maturing concept of [9]cyberterrorism, [10]propaganda and [11]communications online, thus huge amounts of

data to be aggregated and analyzed

- an early warning system for new attack tools, their easy of use, availability, ability to be tracked down, and level of sophistication

- offensive CYBERINT is perhaps the most interesting and aggressive approach I consider fully realistic nowadays.

Operational initiatives such as nation-wide pen testing, OS and IP space mapping for instant exploitation, segmented

economic espionage attacks – [12]ip theft worms achieving efficiency – passive google hacking and reconnaissance,

tensions engineering, zero day vulnerabilities arms race

Outsourcing to [13]objective providers of intelligence and threats data should also be considered, but then

again it's just a tiny portion of what can actually be achieved if a cross-functional team is acting upon a common goal -

to be a step ahead of tomorrow's events, and pleasantly going through threat analysis conducted year ago predicting

and responding to them.

520

If you don't have enemies, it means you're living in a world of idleness, the more they are, the more important is what you're up to.

**Related resources and posts:**

[14]Information Warfare

[15]Cyberterrorism

[16]Intelligence

[17]Benefits of Open Source Intelligence - OSINT

1. <http://en.wikipedia.org/wiki/HUMINT>
2. <http://en.wikipedia.org/wiki/SIGINT>
3. <http://www.fas.org/irp/doddir/army/fm2-22-401.pdf>
4. <http://ddanchev.blogspot.com/2006/05/whos-who-in-cyber-warfare.html>
5. <http://isc.sans.org/packetattack.php>
6. <http://ddanchev.blogspot.com/2006/08/cyber-war-strategies-and-tactics.html>
7. <http://ddanchev.blogspot.com/2006/01/how-to-secure-internet.html>
8. <http://www.cert.org/archive/html/Analysis10a.html>
9. <http://ddanchev.blogspot.com/2006/05/techno-imperialism-and-effect-of.html>
10. [http://ddanchev.blogspot.com/2006/08/cyber-terrorism-communications-and\\_22.html](http://ddanchev.blogspot.com/2006/08/cyber-terrorism-communications-and_22.html)
11. <http://ddanchev.blogspot.com/2006/08/steganography-and-cyber-terrorism.html>
12. <http://www.linuxsecurity.com/docs/malware-trends.pdf>
13. <http://idefense.com/intelligence>

14. <http://del.icio.us/DDanchev/InformationWarfare>
15. <http://del.icio.us/DDanchev/Cyberterrorism>
16. <http://del.icio.us/DDanchev/Intelligence>
17. <http://ddanchev.blogspot.com/2006/09/benefits-of-open-source-intelligence.html>

521

x

## **Examining Internet Privacy Policies (2006-09-18 21:59)**

[1]

Accountability, public commitment, or copywriters charging per word, privacy policies are often taken for

fully enforced ones, whereas the truth is that actually no one is reading, bothering to assess them. And why would

you, as by the time you've finished you'll again have no other choice but to accept them in order to use the service in

question - too much personal and sensitive identifying information is what I hear ticking. That's of course the privacy

conscious perspective, and to me security is a matter of viewpoint, the way you perceive it going beyond the basics,

the very same way you're going to implement it - Identity 2.0 as a single sign on Web is slowly emerging as the real

beast. The marketing perspective, offers unprecedented and fresh data whose value may be the [2]next big project,

balance is the key.

Here's an interesting research on "[3]Examining Internet Privacy Policies Within the Context of Use Privacy Values" :

*" In this paper, we present research bridging the gap between management and software requirements engineering. We address three research questions. 1) What are the most stringently regulated organizations (health care related organizations including health insurance, pharmaceutical, and drugstores) saying in their privacy policy statements? 2) What do consumers value regarding information privacy? 3) Do the privacy policy statements provide the information that consumers want to know?*

*Results from this study can help managers determine the kinds of policies needed to both satisfy user values and ensure privacyaware website development efforts. This paper is organized as follows. First, we discuss relevant research on privacy, policy analysis, and software requirements engineering. Next, we cover the research methodologies of content analysis and survey development, and then the survey results. Finally, we discuss the results and implications of this work for privacy managers and software project managers. "*

The only time privacy policies get read is whenever a [4]leak like [5]AOL's one happens, and mostly for histori-

cal purposes, where's the real value, not the perceived one?  
Don't responsibly generate privacy policies, consider

preemptively appointing [6]chief privacy officers, thus  
committing yourself to valuing your users's privacy and  
having

a strategy in mind.

### **Related resources:**

[7]Privacy

[8]Snooping on Historical Click Streams

[9]A Comparison of US and European Privacy Practices

1.

[http://photos1.blogger.com/blogger/1933/1779/1600/big\\_brother.jpg](http://photos1.blogger.com/blogger/1933/1779/1600/big_brother.jpg)

2. <http://www.google.com/trends>

3.

[http://www4.ncsu.edu/~jbearp/IEEE\\_TEM\\_Privacy\\_Values.pdf](http://www4.ncsu.edu/~jbearp/IEEE_TEM_Privacy_Values.pdf)

4. <http://ddanchev.blogspot.com/2006/08/aols-search-leak-user-4417749.html>

5. <http://ddanchev.blogspot.com/2006/08/aols-search-queries-data-mined.html>

6.

[http://searchsecurity.techtarget.com/originalContent/0,289142,sid14\\_gci1066176,00.html](http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1066176,00.html)

7. <http://del.icio.us/DDanchev/Privacy>

8. <http://ddanchev.blogspot.com/2006/05/snooping-on-historical-click-streams.html>

9. <http://ddanchev.blogspot.com/2006/04/comparison-of-us-and-european-privacy.html>

522

x

## **Results of the Cyber Storm Exercise (2006-09-18 22:01)**

[1]

The [2]Cyber Storm exercise [3]conducted in January "*simulated a sophisticated cyber attack campaign*

*through a series of scenarios directed at several critical infrastructure sectors. The intent of these scenarios was to highlight the interconnectedness of cyber systems with physical infrastructure and to exercise coordination and*

*communication between the public and private sectors. Each scenario was developed with the assistance of industry*

*experts and was executed in a closed and secure environment. Cyber Storm scenarios had three major adversarial*

*objectives:*

- *To disrupt specifically targeted critical infrastructure through cyber attacks*

- *To hinder the governments' ability to respond to the cyber attacks*



*- To undermine public confidence in the governments' ability to provide and protect services"*

Seems like the results from the exercise are [4]already available and among the major findings are related to

:

- Interagency Coordination
- Contingency Planning, Risk Assessment, and Roles and Responsibilities
- Correlation of Multiple Incidents between Public and Private Sectors
- Training and Exercise Program
- Coordination Between Entities of Cyber Incidents
- Common Framework for Response and Information Access
- Strategic Communications and Public Relations Plan
- Improvement of Processes, Tools and Technology

Frontal attacks could rarely occur, as cyberterrorism by itself wouldn't need to interact with the critical infras-

tructure, it would abuse it, use it as platform. However, building confidence within the departments involved is as

important as making them actually communicate with each other.

Go through a previous post on the [5]Biggest Military Hacks of All Time in case you're interested in knowing

more on specific cases related to both, direct and indirect attacks.

1. <http://photos1.blogger.com/blogger/1933/1779/1600/warrior.png>
2. <http://cryptome.org/cyberstorm.ppt>
3. [http://www.dhs.gov/dhspublic/interapp/press\\_release/press\\_release\\_0993.xml](http://www.dhs.gov/dhspublic/interapp/press_release/press_release_0993.xml)
4. [http://www.dhs.gov/interweb/assetlibrary/prep\\_cyberstormreport\\_sep06.pdf](http://www.dhs.gov/interweb/assetlibrary/prep_cyberstormreport_sep06.pdf)
5. <http://ddanchev.blogspot.com/2006/09/biggest-military-hacks-of-all-time.html>

523

x

## **Banking Trojan Defeating Virtual Keyboards (2006-09-19 13:15)**

[1]

The folks behind [2]VirusTotal, just [3]released an [4]analysis and an [5]associated video of trojan generating

video sessions of the infected end user's login process, thus bypassing the virtual keyboard many banks started

providing with the idea to fight keyloggers.

*" Today we will analyze a new banking trojan that is a qualitative step forward in the dangerousness of these*

*specimens and a new turn of the screw in the techniques used to defeat virtual keyboards. The novelty of this trojan lies in its capacity to generate a video clip that stores all the activity onscreen while the user is authenticating to access his electronic bank.*

*The video clip covers only a small portion of the screen, using as reference the cursor, but it is large enough so*

*that the attacker can watch the legitimate user's movements and typing when*

*using the virtual keyboard, so that he gets the username and password without going into further trouble. It would*

*obviously be place a heavy burden on the resources of the computer to capture the complete screen, both when*

*generating the video clip as well as sending it to the attacker. The main reason for doing only a small portion of the screen referenced to the cursor is that the trojan guarantees the speed of the capture to show all the sequence and*

*activity with the virtual keyboard seamlessly. "*

Anything you type can be keylogged, but generating videos of possibly hundreds of infected users would have

a negative effect on the malware author's productivity, which is good at least for now. Follow my thoughts, the

majority of virtual keyboards have static window names, static positions, and the mouse tend to move over X and

Y co-ordinates, therefore doing a little research on the most targeted bank sites would come up with [6]a pattern,

pattern that should be randomized as much as possible. Trouble is, the majority of phishing attacks are still using the static image locations of the banks themselves, when this should have long been randomized as well.

OPIE authentication, suspicious activity based on geotagging anomalies, and transparent process for the customer -

please disturb me with an sms everytime money go out - remain underdeveloped for the time being. You might find

**Candid Wüest's** research on "[7]Phishing in the Middle of the Stream" - Today's Threats to Online Banking informative reading on the rest of the issues to keep in mind.

[8]No Anti Virus Software, No E-banking for You, or are  
[9]Projection Keyboards an alternative?

1.  
[http://photos1.blogger.com/blogger/1933/1779/1600/virtual\\_keyboard.gif](http://photos1.blogger.com/blogger/1933/1779/1600/virtual_keyboard.gif)
2. <http://www.virustotal.com/>
3. <http://blog.hispasec.com/virustotal/8>
4.  
[http://www.hispasec.com/laboratorio/banking\\_trojan\\_capture\\_video\\_clip.pdf](http://www.hispasec.com/laboratorio/banking_trojan_capture_video_clip.pdf)
5.  
[http://www.hispasec.com/laboratorio/troyano\\_video\\_en.htm](http://www.hispasec.com/laboratorio/troyano_video_en.htm)

6. <http://www.devmaster.net/forums/archive/index.php/t-1467.html>

7. <http://www.symantec.com/avcenter/reference/phishing.in.the.middle.of.the.stream.pdf>

8. <http://ddanchev.blogspot.com/2006/05/no-anti-virus-software-no-e-banking.html>

9. <http://www.alpern.org/weblog/stories/2003/01/09/projectionKeyboards.html>

524



## **Soviet Propaganda Posters During the Cold War (2006-09-22 02:06)**

[1]

Posters are a simple, yet influential form of [2]PSYOPS, and their type of one-to-many communication method

successfully achieves a decent viral marketing effect. Here's an [3]archive of Soviet propaganda posters against

the U.S during the Cold War you might find entertaining – here's [4]part 2. **"Capitalists from across the world, unite!"**

[5]North Korea's not lacking behind, and despite the end of the Cold War, is still taking advantage of well

proven and self-serving psychological techniques to further spread their ideology.

Here are some [6]collections of ITsecurity related ones as well.

1.

<http://photos1.blogger.com/blogger/1933/1779/1600/28.jpg>

2. <http://ddanchev.blogspot.com/2006/09/internet-psyops-psychological.html>

3. <http://englishrussia.com/?p=312>

4. <http://englishrussia.com/?p=316>

5. <http://www.dprkstudies.org/documents/nkpics/picgal.html>

6. <http://ddanchev.blogspot.com/2006/02/security-awareness-posters.html>

525

x

## **Airport Security Flash Game (2006-09-22 02:31)**

[1]

Ever wanted to snoop through the luggage of others in exactly the same fashion yours gets searched through?

Try this [2]game, and make sure you keep an eye to the instantly updated "dangerous items" unless you want to be held responsible, and lose your badge.

1.

[http://photos1.blogger.com/blogger/1933/1779/1600/airport\\_security.jpg](http://photos1.blogger.com/blogger/1933/1779/1600/airport_security.jpg)

2. <http://www.shockwave.com/contentPlay/shockwave.jsp?id=airportsecurity&memberStatus=NotSignedIn>

526

## **Interesting Anti-Phishing Projects (2006-09-22 02:56)**

Seven [1]anti-phishing projects, I especially find the browser recon and countermeasures one as a trendy concept, as

phishers are already taking advantage of vulnerabilities allowing them to figure out a browser's history, thus establish a more reputable communication with the victim - adaptive phishing.

### **01. [2]Social Phishing**

*The fundamental purpose of this study was to study the effects of more advanced techniques in phishing using*

*context. Receiving a message from a friend (or corroborated by friends), we hypothesized the credibility of the phishing attempt would be greater*

## **02. [3]Browser Recon and Countermeasures**

*One can use a simple technique used to examine the web browser history of an unsuspecting web site visitor using*

*Cascading Style Sheets. Phishers typically send massive amounts of bulk email hoping their lure will be successful.*

*Given greater context, such lures can be more effectively tailored—perhaps even in a context aware phishing attack*

## **03. [4]Socially Transmitted Malware**

*People are drawn in by websites containing fun content or something humorous, and they generally want to share it*

*with their friends. This is considered social transmission: referral to a location based on recommendation of peers.*

*We measured possible malware spread using social transmission*

## **04. [5]Phishing with Consumer Electronics: Malicious Home Routers**

*It is easy to "doctor" a wireless router like the ones found at home or at a local WiFi hotspot to misdirect legitimate browser links to phoney and often harmful website.*

## **05. [6]Net Trust**

*Individuals are socialized to trust, and trust is a necessary enabler of e-commerce. The human element is the core of*



*confidence scams, so any solution must have this element at its core. Scammers, such as phishers and purveyors of*

*419 fraud, are abusing trust on the Internet. All solutions to date, such as centralized trust authorities, have failed.*

*Net Trust is the solution – trust technologies grounded in human behavior*

## **06. [7]A Riddle**

*Could your browser release your personal information without your knowledge?*

## **07. [8]Phroogle**

*Exploiting comparison shopping engines to bait victims*

You might also be interested in [9]Google's Anti-Phishing Black and White Lists.

1. <http://www.indiana.edu/~phishing/?projects>
2. <http://www.indiana.edu/~phishing/social-network-experiment/>
3. <http://browser-recon.info/>
4. <http://www.verybigad.com/>
5. <http://www.cs.indiana.edu/~atsow/mal-router/>
6. <http://ljean.com/netTrust.html>
7. <http://homer.informatics.indiana.edu/cgi-bin/riddle/riddle.cgi>



*hosting the domain. This is a mission critical service without which the domains in question would be unreachable.*

*Despite the fact that Hizballah is a designated Terrorist entity in the United States, American companies have been, and continue to be the primary providers of service to Hizballah. We now know of 40 domains of Hizballah, based*

*largely on a list provided by Hassan Nasrollah on a previous incarnation of his own web site. Of those 40 domains,*

*23 are now or have been provided DNS services by Alabanza Inc. of Baltimore, Maryland. No other provider comes*

*close. Alabanza's domain name registration business, Bulkregister, is Hizballah's registrar of choice. See our report regarding [3] the registrars of Hizballah's domains. "*

Who knew Hezbollah are indeed the rocket scientists they pretend to be?

[4]UAVs, [5]night vision gear,

[6]SIGINT gear, or has rocket science become so "outsourcable" nowadays?

[7]Cyberterrorism isn't dead, it's just [8]been [9]silently [10]evolving [11]under the [12]umbrella [13]provided

by the mainstream media - wrongly understanding the concept, and [14]stereotyped speculations.

1.

[http://photos1.blogger.com/blogger/1933/1779/1600/23jul06-hizb\\_dns-1024.jpg](http://photos1.blogger.com/blogger/1933/1779/1600/23jul06-hizb_dns-1024.jpg)

2. <http://www.haganah.org.il/harchives/005680.html>

3. <http://www.haganah.org.il/harchives/>
4. <http://ddanchev.blogspot.com/2006/09/hezbollahs-use-of-unmanned-aerial.html>
5. <http://www.sfgate.com/cgi-bin/article.cgi?file=/c/a/2006/08/20/MNGK9KLVH41.DTL>
6. <http://www.defensetech.org/archives/002785.html>
7. <http://www.haganah.org.il/haganah/internet.html>
8. <http://ddanchev.blogspot.com/2006/09/internet-psyops-psychological.html>

528

9. <http://ddanchev.blogspot.com/2006/05/techno-imperialism-and-effect-of.html>
10. [http://ddanchev.blogspot.com/2006/08/cyber-terrorism-communications-and\\_22.html](http://ddanchev.blogspot.com/2006/08/cyber-terrorism-communications-and_22.html)
11. <http://ddanchev.blogspot.com/2006/06/tracking-down-internet-terrorist.html>
12. <http://ddanchev.blogspot.com/2006/08/steganography-and-cyber-terrorism.html>
13. <http://ddanchev.blogspot.com/2006/09/results-of-cyber-storm-exercise.html>
14. <http://ddanchev.blogspot.com/2005/12/cyberterrorism-dont-stereotype-and-its.html>

529

## HP's Surveillance Methods (2006-09-25 02:00)

[1]

Seems like it's not just [2]Board of Directors' Phone Records that were obtained by HP under the excuse of

enforcing an exemplary corporate citizenship, but on pretty much everyone that communicated with them or is

somehow in their circle of friends – no comments on the [3]boring minutes of meetings shared with the press as the

main reason all this. Besides passing the ball to the next board member over who's been aware of, [4]more details

on the exact methods used by HP emerge :

- *HP obtained phone records for seven current or former HP board members, nine journalists, and their family members;*

- *HP provided investigators with the Social Security number of one HP employee, in addition the Social Security numbers of 4 journalists, 3 current and former HP board members, and 1 employee were also obtained by investigators;*

- *HP investigators attempted to use a tracer to track information sent to a reporter;*

- *The concept of sending misinformation to a reporter and the contents of that email were approved by Mr. Hurd,*

*although no evidence was found to suggest that he approved the use of the tracer for surveillance;*

- *Investigators hired by HP monitored a board meeting, a trip to Boulder taken by a board member, as well as the board member's spouse and family members;*

- *In February of 2006, investigators watched a journalist at her residence and in February of 2006 "third party*

*investigators may have conducted a search of an individual's trash."* By the time HP provided the associated parties SSNs, they've pretty much left them on the sharks to finish the rest, disinformation though, is something I previously

thought they didn't do, but with dumpster diving in place as well, I guess they did order the entire all-in-one

surveillance package.

[5]Megacorp ownz your digitally accumulated life, and yes, it can also engineer and snoop on your real one.

All they were so talkative about, is publicly available information that every decent analyst should have definitely

considered starting from HP's historical performance as a foundation for future speculations. In between [6]HP is

(was) also sponsoring a Privacy Innovation Award.

Who's the winner at the bottom line? That's ex-CEO Carly Fiorina - [7]phone records also obtained - whose

upcoming book will [8]profitably take advantage of the momentum.

1.

<http://photos1.blogger.com/blogger/1933/1779/1600/spooka pt.0.gif>

2. <http://ddanchev.blogspot.com/2006/09/hp-spying-on-board-of-directors-phone.html>

3. [http://news.com.com/HP+outlines+long-term+strategy/2100-1014\\_3-6029519.html](http://news.com.com/HP+outlines+long-term+strategy/2100-1014_3-6029519.html)
4. <http://www.redherring.com/article.aspx?a=18730>
5. <http://en.wikipedia.org/wiki/Megacorporation>
6. <http://abcnews.go.com/Technology/wireStory?id=2474537>
7. [http://www.mercurynews.com/mld/mercurynews/news/breaking\\_news/15551547.htm](http://www.mercurynews.com/mld/mercurynews/news/breaking_news/15551547.htm)
8. [http://www.businessweek.com/technology/content/sep2006/tc20060921\\_455418.htm](http://www.businessweek.com/technology/content/sep2006/tc20060921_455418.htm)

530

x

## **Able Danger's Intelligence Unit Findings Rejected (2006-09-25 02:44)**

[1]

The much hyped [2]Able Danger [3]Intelligence unit which has supposedly collected and identified information

on the 9/11 terrorist attacks [4]claim was officially rejected :

*The report found that the recollections of most of the witnesses appeared to focus on a "single chart depicting*

*Al Qaeda cells responsible for pre-9/11 terrorist attacks" that was produced in 1999 by a defense contractor, the Orion Scientific Corporation.*

*While witnesses remembered having seen Mr. Atta's photograph or name on such a chart, the inspector gen-*

*eral said its investigation showed that the Orion chart did not list Mr. Atta or any of the other Sept. 11 terrorists, and that "testimony by witnesses who claimed to have seen such a chart varied significantly from each other." The report says that a central witness in the investigation, an active-duty Navy captain who directed the Able Danger program,*

*had changed his account over time, initially telling the inspector general's office last December that he was "100*

*percent" certain that he had seen "Mohamed Atta's image on the chart."*

### **Issues to keep in mind:**

- the chaotic departmental information sharing or the lack of such, budget-deficit arms race, thus departments

wanting to get credited for anything ground breaking

- prioritizing is sometimes tricky, wanting to expand a node, thus gather more intelligence and more participants

might have resulted in missing the key ones, marginal thinking fully applies

- [5]OSINT as this [6]Social Network Analysis of the 9-11 Terror Network shows, is [7]an invaluable asset and so is the

momentum and actual use of the data

Despite that if you don't have a past, you're not going to have a future, true leaders never look into the past,



they shape the future and don't mind-tease what they could have done. Necessary evil moves the world in its own

orbit now more than ever, and if you really don't have a clue what I'm trying to imply here, then you're still not ready for that mode of thinking.

So, [8]the man who knew, but no one reacted upon his findings in a timely manner, or a case-study of how

terrabbytes of mixed OSINT and Intelligence data weren't successfully [9]data mined? I go for the first point.

Able Danger chart courtesy of the [10]Center for Cooperative Research.

1. [http://photos1.blogger.com/blogger/1933/1779/1600/501\\_able\\_danger\\_chart.jpg](http://photos1.blogger.com/blogger/1933/1779/1600/501_able_danger_chart.jpg)
2. <http://www.abledangerblog.com/>
3. [http://en.wikipedia.org/wiki/Able\\_Danger](http://en.wikipedia.org/wiki/Able_Danger)
4. <http://www.nytimes.com/2006/09/22/us/22able.html?ref=us>
5. <http://ddanchev.blogspot.com/2006/09/benefits-of-open-source-intelligence.html>
6. <http://www.orgnet.com/prevent.html>
7. <http://ddanchev.blogspot.com/2006/05/terrorist-social-network-analysis.html>
8. <http://www.pbs.org/wgbh/pages/frontline/shows/knew/etc/connect.html>

9. <http://ddanchev.blogspot.com/2006/03/data-mining-terrorism-and-security.html>

10. <http://www.cooperativeresearch.org/searchResults.jsp?searchtext=able+danger&events=on&entities=on&articles=on&topics=on&timelines=on&projects=on&titles=on&descriptors=on>

531

x

## **Terrorism and Response 1990-2005 (2006-09-25 03:56)**

[1]

Very informative and objective retrospective on the response to terrorism from 1990 to 2005. The [2]syllabus

by Bruce D. Larkin and Ben Lozano is even more resourceful with its "what if" brainstorming questions.

Here's another [3]map of terrorist networks in America for 1991-2005, based on states and possible cell of

operation - two more previous [4]versions [5]available.

1. <http://photos1.blogger.com/blogger/1933/1779/1600/Terrorism.1990-2006.png>

2. <http://www.learnworld.com/COURSES/P72/P72.Syllabus.html>

3. <http://www.dickdestiny.com/blog/2006/09/united-states-of-al-qaeda-terrorists.html>

4.

[http://www.doglegs.net/cclovett/9/Terrorist\\_Map\\_of\\_the\\_US.jpg](http://www.doglegs.net/cclovett/9/Terrorist_Map_of_the_US.jpg)

5.

<http://www.homelandsecurityus.net/images/terrorist%20network%20in%20america.bmp>

532

x

## **Media Censorship in China - FAQ (2006-09-27 12:23)**

[1]

Controversial to the generally accepted perspective that [2]China's Internet censorship efforts are [3]primarily

a [4]technological solution only, I feel it's self-regulation as a state of mind that's having the greatest impact on the success of their efforts – the very same way you're being told not to misbehave while seeing yourself on a monitor

when entering a store for instance. [5]Self-censorship as a state of mind by itself is a way of hiding the plain truth

that the Chinese government is aware it cannot fully control what information is coming in, and going out of the

country. That of course doesn't stop it from speculating it still can. Here's a recent [6]FAQ on the Media Censorship

in China answering the following questions :

[7]What is the current media policy in China?

[8]How free is Chinese media?

[9]What are the primary censoring agencies in China?

[10]How does China exert media controls?

[11]How does China control the influence of foreign media?

[12]How do journalists get around media control measures?

The main agencies responsible for history engineering :

*" But the most powerful monitoring body is the Communist Party's Central Propaganda Department (CPD), which*

*coordinates with GAPP and SARFT to make sure content promotes and remains consistent with party doctrine. Xinhua,*

*the huge state news agency (7,000 employees, according to official statistics), is beholden to the CPD and therefore considered by press freedom organizations to be a propaganda tool. The CPD gives media outlets directives restricting coverage of politically sensitive topics—such as protests, environmental disasters, Tibet, and Taiwan—which could be considered dangerous to state security and party control. "*

Centralization as the core of control, why am I not surprised?  
Don't tolerate [13]censorship, learn [14]how to

undermine it.

1.

<http://photos1.blogger.com/blogger/1933/1779/1600/Censorship.1.jpg>

2. <http://ddanchev.blogspot.com/2006/02/chinese-internet-censorship-efforts.html>

3. <http://ddanchev.blogspot.com/2006/07/chinas-interest-of-censoring-mobile.html>
4. <http://ddanchev.blogspot.com/2006/08/chinas-internet-censorship-report-2006.html>
5. <http://ddanchev.blogspot.com/2006/07/south-koreas-view-on-chinas-media.html>
6. <http://www.cfr.org/publication/11515/>
7. <http://www.cfr.org/publication/11515/#2>
8. <http://www.cfr.org/publication/11515/#3>
9. <http://www.cfr.org/publication/11515/#4>
10. <http://www.cfr.org/publication/11515/#5>
11. <http://www.cfr.org/publication/11515/#6>
12. <http://www.cfr.org/publication/11515/#7>
13. <http://del.icio.us/DDanchev/Censorship>
14. <http://irrepressible.info/>

533

x

## **Afterlife Data Privacy (2006-09-27 13:36)**

[1]

Have you ever asked yourself what's going to happen with your digital data in case the worst happens, or

most importantly, the pros and cons of privacy in such a situation?

[2] Taking passwords to the grave is always be default, and while your email service provider may get socially

engineered – or have to comply with a court order – under the excuse of emotional crisis, family relations, reconsider

how you would like to have your (accounting) data handled :

*" The situation poses a dilemma for e-mail providers that are pilloried by privacy rights advocates at the mere suggestion of sensitive data being exposed, at the same time they are expected to hand over the digital keys to family members when a customer dies. Last year, Yahoo was forced to provide access to the e-mail of a U.S. Marine killed*

*in Iraq to his father, [3] who got a court order in the matter.*

*"The commitment we've made to every person who signs up for a Yahoo Mail account is to treat their e-mail as a private communication and to treat the content of their messages as confidential," said Yahoo spokeswoman Karen Mahon.*

*Beyond acknowledging that Yahoo complies*

*with court orders, Mahon declined to discuss Yahoo's requirements for providing family members access to the e-mail*

*accounts of their deceased loved ones. Google will provide access to a deceased Gmail user's account if the person*

*seeking it provides a copy of the death certificate and a copy of a document giving the person power of attorney over the e-mail account, said a Google spokeswoman. "*

Whereas some inboxes should never be opened – your spouse’s one for instance – leading email providers have already established practices when dealing with such requests and I feel the lack of reliable stats on the occurrences of such isn’t proving the necessary discussion. The majority of people I know don’t just have a black and white sides of their characters, they’re too colorful to hide it both offline and online, and that’s what makes them "people I know". Changing a [4]provider’s privacy policy wouldn’t necessarily have a significant effect unless an author’s email communication truly becomes his property, while on the other hand local laws could ruin the effect.

It would be highly flexible if users are offered the opportunity to speak for themselves and their [5]privacy while still able to do it.

Sometimes, on your journey to happiness and emotional balance you end up opening more and more of Pandora’s boxes, when what you’re looking for is right inside your head - the clear memory of the person in question, not the pseudo-individuality in all of its twisted variations. Make sure what you wish for, as it may actually happen!

The ultimate question - [6]Why does a deceased soldier’s email thoughts become the property of a company?

1.

<http://photos1.blogger.com/blogger/1933/1779/1600/VR.0.jpg>

2.

[http://news.com.com/Taking+passwords+to+the+grave/2100-1025\\_3-6118314.html](http://news.com.com/Taking+passwords+to+the+grave/2100-1025_3-6118314.html)

3. [http://news.com.com/Yahoo+releases+e-mail+of+deceased+Marine/2100-1038\\_3-5680025.html?](http://news.com.com/Yahoo+releases+e-mail+of+deceased+Marine/2100-1038_3-5680025.html?tag=nl)

[tag=nl](http://news.com.com/Yahoo+releases+e-mail+of+deceased+Marine/2100-1038_3-5680025.html?tag=nl)

4. <http://ddanchev.blogspot.com/2006/09/examining-internet-privacy-policies.html>

5. <http://del.icio.us/DDanchev/Privacy>

6.

<http://exlibris.memphis.edu/ethics21/archives/05eei/papers/lois.pdf>

534

x

## **Anti-Counterfeiting Technologies (2006-09-28 00:47)**

[1]

Handy [2]overview of various anti-counterfeiting technologies and where they're primarily used at, such as

Holograms, Optically variable inks, Microlenticular technology, Special inks, Nanomarkers, and yes, RFID tags, but

keep in mind that they used to be "covert" decades ago, but in the passports of some nowadays.

You might find a previous post "[3]Pass the Scissors" worth reading as well.



1. [http://photos1.blogger.com/blogger/1933/1779/1600/ten\\_bu\\_cks.jpg](http://photos1.blogger.com/blogger/1933/1779/1600/ten_bu_cks.jpg)
2. [http://www.csoonline.com/read/090106/brf\\_anti-counterfeit.html](http://www.csoonline.com/read/090106/brf_anti-counterfeit.html)
3. <http://ddanchev.blogspot.com/2006/05/pass-scissors.html>

535

x

## **NSA Mind Control and PSYOPS (2006-09-28 01:02)**

[1]

Basics of recruiting, interrogations, [2]brainwashing and [3]PSYOPS on the foundations of Visual Hallucinations,

Event-Triggered (conditional) Implant Delivery, and Complete Quiet Silence? Maybe, but this [4]article is full of

interesting concepts, consider however skipping the part on how the NSA brainwashed Curt Cobain :

*" Curt Cobain of the musical group "Nirvana" was another victim of NSA brainwashing and was terminated by NSA. Cobain had started writing clues to the NSA activities into his music to communicate it to his music followers. He referred in music to the NSA as the "Friends inside his head". Once the NSA puts on the highest level of brainwashing pain, the subject expires quickly. Cobain used heroin to numb and otherwise slow the effect of the brainwashing. "*

He had different "[5]friends".

**Related resources:**

[6]Intelligence

[7]NSA

1. <http://photos1.blogger.com/blogger/1933/1779/1600/nsa.jpg>
2. <http://en.wikipedia.org/wiki/Brainwashing>
3. <http://ddanchev.blogspot.com/2006/09/internet-psyops-psychological.html>
4. <http://www.whale.to/b/nsa4.html>
5. [http://en.wikipedia.org/wiki/Curt\\_cobain#Cobain.27s\\_final\\_weeks](http://en.wikipedia.org/wiki/Curt_cobain#Cobain.27s_final_weeks)
6. <http://del.icio.us/DDanchev/Intelligence>
7. <http://del.icio.us/DDanchev/NSA>

536

x

## **Satellite Imagery of Secret or Sensitive Locations (2006-09-28 02:12)**

[1]

Continuing the [2]Travel Without Moving Series, and a previous post on [3]Open Source North Korean IMINT

Reloaded, this collection of Google Earth, Google Maps, Local Live and Yahoo Maps versions of [4]secret or sensitive

locations is worth browsing through. Included coordinates for over 80 locations, for instance :

- Predator Drone Returning From Mission
- Predator Drones at Remote Airstrip
- Predator Drone Taking Off From Remote Airstrip
- TAGS 45 'Waters'
- M80 'Stiletto' Stealth Boat
- U-2 Being Readied For Mission
- Underground Hangars at Sunchon Airbase
- North Korean No-Dong Missile Assembly Building
- Former MI6/FCO high security SIGINT enclave at Poudon
- Former NSA/DoD satellite intercept site
- CIA 'Black Site' for terrorist interrogations
- Russian Foreign Intelligence (SVR) Headquarters
- CFS Leitrim - Satellite Signal Interception station
- Russian Don-2NP Pill Box Radar
- Star Wars missile defense support site
- AN/FRD-10 Classic Bullseye Antenna
- Radomes on Fort Belvoir
- Northrop "Secret" Research Facility
- Classic Bullseye listening antenna array

As you will find out the data provided is a historical one – the UAVs and B2s have already disappeared for in-

stance. Does the publicly obtainable imagery represent a threat to these locations? Not necessarily, as threats

from which these facilities were supposed to be protected from have been replaced by ones requiring a different

perspective. The dishes however, are still there, listening..

### **Related posts and resources:**

[5]Satellite

[6]Defense

[7]Military

[8]Japan's Reliance on U.S Spy Satellites and Early Warning Missile Systems

[9]Stealth Satellites Developments Source Book

[10]Anti Satellite Weapons

1.  
<http://photos1.blogger.com/blogger/1933/1779/1600/9422.jpg>

2. <http://ddanchev.blogspot.com/2006/07/travel-without-moving-north-korea.html>

3. <http://ddanchev.blogspot.com/2006/07/open-source-north-korean-imint.html>

4.  
<http://virtualglobetrotting.com/category/buildings/covert/0/?>

[v=0&f=0&so=1](#)

5. <http://del.icio.us/DDanchev/Satellite>
6. <http://del.icio.us/DDanchev/Defense>
7. <http://del.icio.us/DDanchev/Military>
8. <http://ddanchev.blogspot.com/2006/07/japans-reliance-on-us-spy-satellites.html>
9. <http://ddanchev.blogspot.com/2006/09/stealth-satellites-developments-source.html>
10. <http://ddanchev.blogspot.com/2006/08/anti-satellite-weapons.html>

537

x

## **Government Data Mining Programs - Interactive (2006-09-28 02:56)**

[1]

A very [2]extensive visualization of various U.S government data mining programs :

*" Individually, each piece of information gives only a small glimpse into people's lives – but over time, these bits of personal information can begin to reveal patterns. Such as the places they go, the products they buy, or*

*perhaps the type of people they associate with. This pattern-recognition process is called "Data Mining" or sometimes*

*"Knowledge Discovery." Since September 11, the federal government – especially intelligence and law enforcement*

*agencies – have turned to data mining programs to make sense of growing oceans of data. The end result isn't*

*always about discovering what people have done – but what people might do tomorrow. What does a terrorist look*

*like? What is the culmination of their credit, contacts, purchases and travel? Is it possible that you might share these similar patterns? Chances are at least some of these programs sift through personal information about you. "*

Go through the questionnaire for a specific case, directly on a program of interest and see its relationship

with the rest, if any of course. Go through a previous post on [3]Able Danger's Intelligence Unit Findings Rejected to

find out more about the state of information sharing.

1.

[http://photos1.blogger.com/blogger/1933/1779/1600/data\\_mining\\_interactive.0.jpg](http://photos1.blogger.com/blogger/1933/1779/1600/data_mining_interactive.0.jpg)

2.

[http://newsinitiative.org/story/2006/09/01/government\\_data\\_mining\\_programs](http://newsinitiative.org/story/2006/09/01/government_data_mining_programs)

3. <http://ddanchev.blogspot.com/2006/09/able-dangers-intelligence-unit.html>

538

## **2.10 October**

539

## **Mark Hurd on HP's Surveillance and Disinformation (2006-10-04 18:22)**

[1]

Straight from the source - HP's CEO, one that compared to Fiorina's qualitative approaches decided to shift the

company's strategy to a quantitative internal benchmarking model - one is always fulfilling the other and vice versa -

and he succeeded, but with today's competitive environment and seek for "the next big thing" some companies are sacrificing productivity for insider fears related investigations. [2]Not that there aren't any, it's just that this particular case is nothing more than a bored top management employee sending signals to the press. Next time it would

be a top floor hygiene COO's comments on how HP are definitely up to something given the late hour conference

meetings, the press will quote as "an insider source leaked this to us" type of quotation :

*" Now the question is do you pick up the document and turn to page whatever, or do you say, 'are you sure?'*

*He says 'I'm sure.' So then you say, 'what are we going to do?' Now let me give you two thoughts. You could react*

*by not confronting the problem. You talk about ethics. We've gone down the backward looking view. There's also*

*the dimension that says, are you going to bury this or confront it. Pretty big question, right? And I want to make*

*something clear. I only know of the facts around the one leak. I don't know, there's been a lot of speculation around tens of leaks, and they associate with this one person [Jay Keyworth, a longtime HP board member]. This fact was*

*about one leak from this one person who is a really good guy in the sense of contributions he made to Hewlett Packard over many years.*

*So now you're confronted with data that says, great contributor, and the team is looking at Pattie [Then board*

*chairman Patricia Dunn] and saying 'what are you going to do.' And I can tell you if you're looking down at this room as you're making a decision, my first reaction wasn't to say, 'hey Pattie, why don't you look backward at how the*

*data was collected.' The stress was, how are you going to confront the fact that was being presented to you. You're*

*going to do what?*

*Now to your point, knowing what we know now I wish we'd looked at a different set of facts. But even at that*

*point, what had been done had been done. You'd have been reacting at that point in time. I don't want to shirk any*

*of this. The buck stops with me. But you can't have a CEO of a company our size being the backstop. The thought*

*that I'm going to catch everything - revenue, costs, personnel decisions, investigations... you know the scale of this company. "*

Catch up with the case through a [3]previous post on the topic, and [4]keep on [5]reading.



1. [http://money.cnn.com/2006/09/29/technology/pluggedin\\_lashinsky\\_hurd.fortune/index.htm?section=money\\_technology](http://money.cnn.com/2006/09/29/technology/pluggedin_lashinsky_hurd.fortune/index.htm?section=money_technology)
2. <http://ddanchev.blogspot.com/2005/12/insiders-insights-trends-and-possible.html>
3. <http://ddanchev.blogspot.com/2006/09/hp-spying-on-board-of-directors-phone.html>
4. <http://del.icio.us/DDanchev/Surveillance>
5. <http://del.icio.us/DDanchev/Privacy>

540



## **Filtering "Good Girls" and IM Threats (2006-10-05 15:21)**

[1]

Respecting your kids' right to privacy while wanting to ensure you're aware of the

type of people they IM with? Consider a recently launched initiative, [2]IMSafer aims to filter, not spy on kids :

*" Keeping children safe from predatory adults in online communication is a service in high demand, but in order for children to participate the parental control needs to be kept to a minimum. [3] IMSafer is a service that launched today and promises to filter IM communication for conversation deemed potentially predatory. The company says it worked with law enforcement specialists to develop its filtering rules and some of them are quite interesting - the phrase "you're a good girl" is believed to be common language for building a dominance/submission based relationship, for example. Only questionable excerpts from IM conversations will be shown to parents; the company hopes that this relative privacy will help buy-in from kids. "*

Yet, this is a great example of marginal thinking when it comes to detecting potential child abuse activities

with respect to little princess's - why not prince? - right to digital privacy. Whereas in the spirit of Web 2.0, the

concept is primarily driven by the collective wisdom of parents participating and shaping the service's database and

increasing interactions, IMSafer has already [4] predefined categories of alerts :

*" 1. Someone looking to make direct contact (i.e. coming to your house)*

*2. Someone looking to make indirect contact (i.e. calling a phone)*

*3. Personal information (i.e. phone numbers)*

*4. Obscene language*

*5. Specific and sexual references to body parts*

*6. Specific references to sexual acts*

*7. Anything related to pedophilia"*

### **Issues to keep in mind :**

- the differently perceived dangerous or offensive conversation by parents

- the presumption that the "predator" would be using the same username next time, thus establishing long-lasting reputation

- how kids feeling in the middle of a silent war with their parents could simply IM from another location, one without

the software installed excluding the possibilities of bypassing it with nerdy talk or vulnerabilities and hacks appearing on-the-fly

- monitors IM only, thus email, IRC, and forums remain an option for further communication

Don't emphasize on spying, not even filtering, but on educating your kids, thus gaining their participation in

the process of building awareness on what's are potentially dangerous IM activities. From another perspective, do

bored or adventurous kids spend time chatting with strangers? I think boringness, loneliness, the lack of strong, even

developed communications with their folks is the root of the problem. And yes, predators acting as online stalkers,

541

thus improving their chances of utilizing a long-lasting conversation.

### **Related posts:**

[5]What's the potential of the IM security market? Symantec thinks big

[6]"IM me" a strike order

1.

[http://photos1.blogger.com/blogger/1933/1779/1600/sheep\\_wolf.gif](http://photos1.blogger.com/blogger/1933/1779/1600/sheep_wolf.gif)

2. <http://www.techcrunch.com/2006/10/03/imsafer-filters-not-spies-on-kids/>

3. <http://imsafer.com/>

4. <http://imsafer.com/splash/faq>

5. <http://ddanchev.blogspot.com/2006/01/whats-potential-of-im-security-market.html>

6. <http://ddanchev.blogspot.com/2006/04/im-me-strike-order.html>

542



## **Terrorist Letters and Internet Intentions (2006-10-05 15:49)**

[1]

A juicy recently [2]de-classified letter to Zarqawi courtesy of the [3]Combating Terrorism

Center, reveals possible intentions for Internet based communications :

*" We advise you to maintain reliable and quick contact, with all the power you can muster. **I am ready to com-***

***municate via the Internet or any other means, so send me your men to ask for me on the chat forum of Ana***

***al-Muslim, or others. The password between us is that thing that you brought to me a long time ago from Herat.***

*Then, after that, we would agree with them about e-mails, or you should instruct your men who are in the country*

*that I live in to develop communications with us. We are ready to write to you and to consult with you regarding*

*opinions anytime directly. "By the time, Surely man is at a loss, Except for those who believe and do good, and exhort one another to Truth, and exhort one another to patience. "*

Rather primitive suggestion [4]compared to the [5]alternatives, it sounds more of a loyal jihadist trying to demonstrate his determination of making an impact. The other day I came across to an article mentioning the possibility of "[6]suicidal hackers", that is hackers who doesn't care whether they'll be caught or not in a possible information warfare scenario - [7]chinese hackers have been utilizing the power of masses, thus disinforming on the actual sophistication

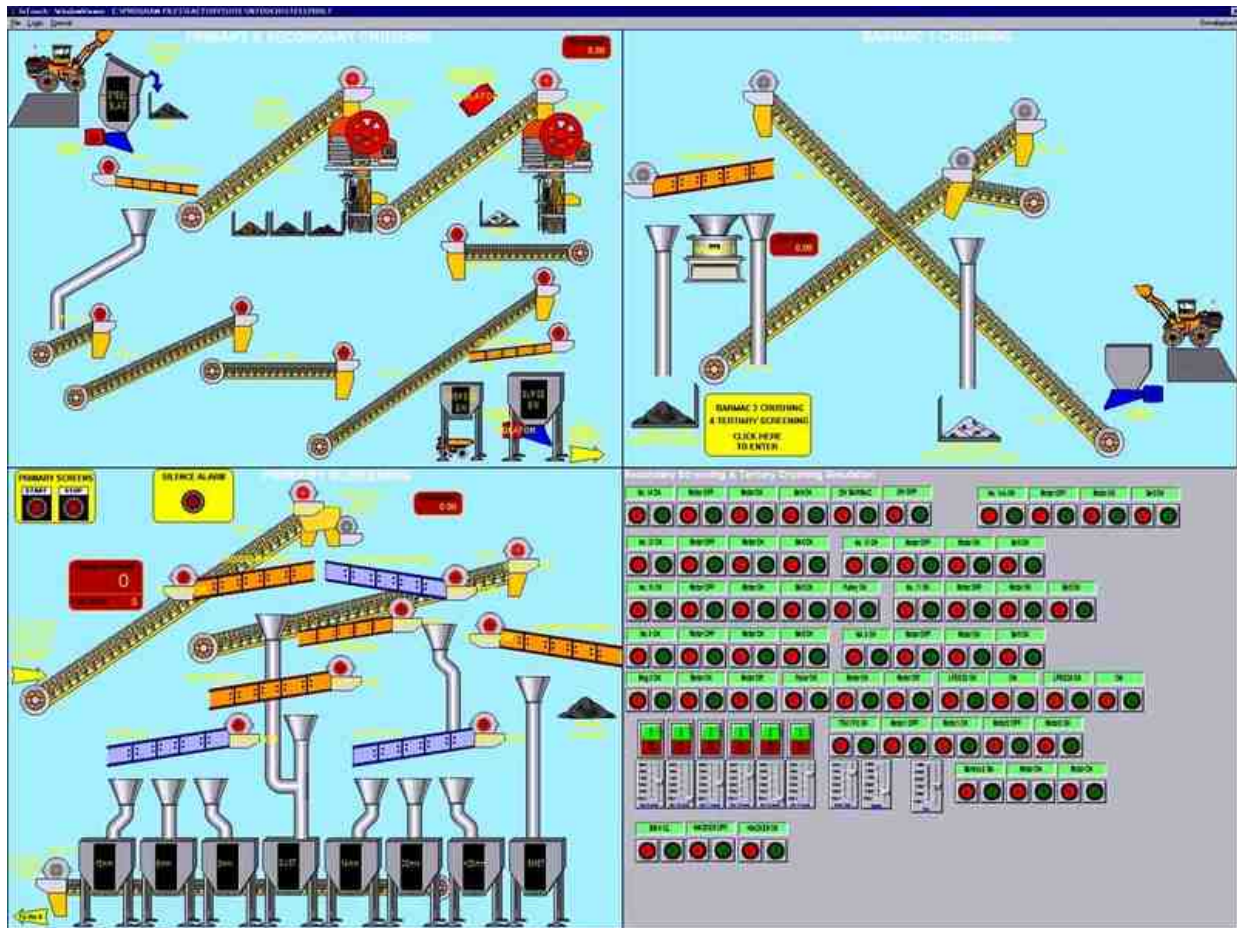
of the attack and directing the traceback efforts to script kiddies.

However, in this case that's an example of a suicidal jihadist.

1. <http://photos1.blogger.com/blogger/1933/1779/1600/female-suicide-bomb.jpg>
2. <http://www.ctc.usma.edu/harmony/CTC-AtiyahLetter.pdf>
3. <http://www.ctc.usma.edu/harmony.asp>
4. [http://ddanchev.blogspot.com/2006/08/cyber-terrorism-communications-and\\_22.html](http://ddanchev.blogspot.com/2006/08/cyber-terrorism-communications-and_22.html)
5. <http://ddanchev.blogspot.com/2006/08/steganography-and-cyber-terrorism.html>
6. [http://www.zdnet.com.au/news/security/soa/Army\\_expects\\_suicide\\_hacker\\_attacks/0,130061744,339271362,00.htm](http://www.zdnet.com.au/news/security/soa/Army_expects_suicide_hacker_attacks/0,130061744,339271362,00.htm)

7. <http://ddanchev.blogspot.com/2006/09/chinese-hackers-attacking-us.html>

543



## SCADA Security Incidents and Critical Infrastructure Insecurities (2006-10-05 16:21)

[1]

A [2]decent article on the topic of the most hyped [3]cyberterrorism threat of them all - direct attack on the critical

infrastrcture of a country by [4]attacking the SCADA devices - despite increased connectivity and integration with

third-party networks, for the time being misconfigurations and failures in maintenance make their impact. What is

critical infrastructure anyway? In the days when it used to be a closed network, that is one isolated from the Internet

and performance-obsessed top management, dealing with threats was benefiting from the controlled environment

compared to the open Internet. Converging both infrastructures to maximize performance, project demand and

supply, thus achieving cost-cutting and profits results in the basic truth that polluting the Internet would inevitably

influence the what used to be closed critical infrastructure one – and it [5]already happened on several occasions.

Incident in Australia :

*" That was the case in Australia in April 2000. Vitek Boden, a former contractor, took control of the SCADA*

*system controlling the sewage and water treatment system at Queensland's Maroochy Shire. Using a wireless*

*connection and a stolen computer, Boden released millions of gallons of raw sewage and sludge into creeks, parks*

*and a nearby hotel. He later went to jail for two years. Not surprisingly, U.S. companies are hesitant to talk about the security of their SCADA networks for fear they may give clues to hackers. But security consultants say problems with them are widespread. Allor's company, for instance, regularly does audits of SCADA systems at major installations*



*such as power plants, oil refineries and water treatment systems.*

*Almost invariably, Allor said, the companies claim their SCADA systems are secure and not connected to the*

*Internet. And almost invariably, he said, ISS consultants find a wireless connection that company officials didn't know* 544

*about or other open doors for hackers. Realizing the growing threat, the federal government two years ago directed its Idaho National Laboratory to focus on SCADA security. The lab created the nation's first "test bed" for SCADA networks and began offering voluntary audits for companies. "*

And more security incidents courtesy of Filip Maertens -  
[6]Cyber threats to critical infrastructures slides :

**1992** – Chevron – Emergency system was sabotaged by disgruntled employee in over 22 states

**1997** – Worchester Airport – External hacker shut down the air and ground traffic communication system for six  
hours

**1998** – Gazprom – Foreign hackers seize control of the main EU gas pipelines using trojan horse attacks

**2000** – Queensland, Australia – Disgruntled employee hacks into sewage system and releases over a million liters of raw sewage into the coastal waters

**2002** – Venezuela Port – Hackers disable PLC components during a national unrest and general workers strike,

disabled the country's main port

**2003** – U.S East Coast blackout – A worm did not cause the blackout, yet the Blaster worm did significantly infect all systems that were related to the large scale power blackout

**2003** – Ohio Davis-Besse Nuclear Plant – Plant safety monitoring system was shut down by the Slammer worm for over five hours

**2003** – Israel Electric Corporation – Iran originating cyber attacks penetrate IEC, but fail to shut down the power grid using DoS attacks

**2005** – Daimler Chrysler – 13 U.S manufacturing plants were shut down due to multiple internet worm infections

(Zotob, RBot, IRCBot)

**2005** – International Energy Company – [7]Malware infected HMI system disabled the emergency stop of equipment

under heavy weather conditions

**2006** – Middle East Sea Port – Intrusion test gone wrong. ARP spoofing attacks shut down port signaling system

**2006** – International Petrochemical Company – Extremist propaganda was found together with text files containing

usernames & passwords of control systems

Go through the [8]results of the Cyberstorm cyber exercise, and a previous post on [9]The Biggest Military

Hacks of All Time to grasp the big picture of what [10]cyberterrorism and [11]asymmetric warfare is all about.

1. <http://photos1.blogger.com/blogger/1933/1779/1600/scada.jpg>
2. <http://www.ajc.com/business/content/business/stories/2006/10/02/1001sbizscada.html>
3. <http://del.icio.us/DDanchev/Cyberterrorism>
4. <http://del.icio.us/DDanchev/SCADA>
5. <http://www.computerworld.com/securitytopics/security/recovery/story/0,10801,84510,00.html>
6. [http://www.uniskill.be/downloads/UNISKILL\\_2006\\_-\\_ECSA\\_-\\_SCADA\\_Security\\_v\\_1.0.pdf](http://www.uniskill.be/downloads/UNISKILL_2006_-_ECSA_-_SCADA_Security_v_1.0.pdf)
7. <http://www.linuxsecurity.com/docs/malware-trends.pdf>
8. <http://ddanchev.blogspot.com/2006/09/results-of-cyber-storm-exercise.html>
9. <http://ddanchev.blogspot.com/2006/09/biggest-military-hacks-of-all-time.html>
10. <http://ddanchev.blogspot.com/2006/05/techno-imperialism-and-effect-of.html>
11. <http://www.blackhat.com/presentations/bh-federal-06/BH-Fed-06-Maynor-Graham-up.pdf>

545

x

**Automated SEO Spam Generation (2006-10-12 13:27)**

[1]

In a previous post "[2]An Over-performing Spammer" I commented an impossible to both, read and detect

scam message – loading remote email images is both, an infection and privacy exposing vector. In case you also

remember [3]automated bots were also self-praising themselves over Ebay back in August.

Just noticed a [4]good example ( <http://hsbc-internet-banking.1st-results-links-resource-7.info/No-Anti-Virus->

[Software-No-E-Banking-For-You/](http://hsbc-internet-banking.1st-results-links-resource-7.info/No-Anti-Virus-Software-No-E-Banking-For-You/) ) of automated SEO spam generated page out of my "[5]No Anti-Virus Software, No

E-banking For You" post :

*" Welcome to the No Anti Virus Software No E Banking For You one stop website! We offer the best informa-*

*tion, resources and links on this side of the planet, you will find no greater and more comprehensive source for all your No Anti Virus Software No E Banking For You needs! ONLY at our website, will you find every Top Quality information*

*and knowledge resource website on the No Anti Virus Software No E Banking For You topic! Please Enjoy your stay at*

*your #1 No Anti Virus Software No E Banking For You website, and do remember to bookmark, come again and tell all*

*your friends! "*

While it's amusing, Google seems to have already picked up the now disappeared subdomain. I wonder when,

and would Google utilize the "wisdom of crowds" concept when it comes to users signaling such search results the way it's already flagging blogs? From another perspective, web application vulnerabilities in domains Google's very

found of have the potential to undermine any web site rating initiative. Such spam pages aren't the big problem, the

big problem is an ecosystem that allows the author to take advantage of the "upcoming search traffic" on a topic while taking advantage of a marketing window of an event to abuse.

1.

<http://photos1.blogger.com/blogger2/4099/2257/1600/NoSpam.gif>

2. <http://ddanchev.blogspot.com/2006/06/over-performing-spammer.html>

3. <http://ddanchev.blogspot.com/2006/08/but-of-course-its-pleasant-transaction.html>

4. [http://209.85.129.104/search?q=cache:tonLpQFObrwJ:hsbc-internet-banking.1st-results-links-resource-7.info/](http://209.85.129.104/search?q=cache:tonLpQFObrwJ:hsbc-internet-banking.1st-results-links-resource-7.info/No-Anti-Virus-Software-No-E-Banking-For-You/)

[No-Anti-Virus-Software-No-E-Banking-For-You/](http://209.85.129.104/search?q=cache:tonLpQFObrwJ:hsbc-internet-banking.1st-results-links-resource-7.info/No-Anti-Virus-Software-No-E-Banking-For-You/)

5. <http://ddanchev.blogspot.com/2006/05/no-anti-virus-software-no-e-banking.html>

546

## **The Insider's Guide to Georgia-Russia Espionage Case (2006-10-12 14:26)**

[1]

An [2]informative FAQ on the most recent nation-2-nation espionage case, David vs Goliath aka Georgia's

counter-intelligence services spotting Russian military personnel performing HUMINT reconnaissance under Russia's

umbrella. It answers the following questions :

- Russian spies in Georgia? I thought some of the folks in Atlanta looked a bit suspicious...**
- So what's the problem this week?**
- And did Georgia back down?**
- What were four Russian military officers doing in Tblisi in the first place?**
- Anything else they're unhappy about?**
- Is the situation likely to escalate any further?**

What happened actually? Russia is very interested in its post-soviet era "satellites" and their ongoing and upcoming activities with NATO, and yes, the U.S interest in breaking the ice by organizing various military exercises,

even worse from Russia's point of view - opening military bases and a country's airspace to the U.S Air Force. Russia

was basically underestimating Georgi's capabilities, sensitivity to the reconnaissance, and courage to go public with

the findings if any, and later on acted as a wounded 800 pound gorilla feeling embarrassed.

Meanwhile, who's been [3]killing all these journalists - 42 since 1992 - acting as the society's watchdog, and

was Anna Politkovskaya assassination on purposely done on Vladimir Putin's birthday to destabilize the public opinion

on the government's capability to solve the case, and open up countless speculations on the similarities between

[4]Georgi Markov's case who was also killed on a puppet's birthday?

It's the typical Fox Mulder situation, he knows everything about you, you know everything about him, do

something to him and make him a hero of a cause, so I feel organized crime isn't interested in Russia's social

accountability and is destabilizing the process.

### **Related posts and resources:**

[5]Prosecuting Defectors and Appointing Insiders

[6]A top level espionage case in Greece

[7]India's Espionage Leaks

[8]Intelligence

[9]Espionage

1.

[http://photos1.blogger.com/blogger/1933/1779/1600/david\\_vs\\_goliath.jpg](http://photos1.blogger.com/blogger/1933/1779/1600/david_vs_goliath.jpg)

2. <http://edition.cnn.com/2006/WORLD/europe/10/02/insider.georgia/index.html>
3. [http://www.pbs.org/newshour/bb/media/july-dec06/russia\\_10-09.html](http://www.pbs.org/newshour/bb/media/july-dec06/russia_10-09.html)
4. <http://ddanchev.blogspot.com/2006/06/travel-without-moving-georgi-markovs.html>
5. <http://ddanchev.blogspot.com/2006/09/prosecuting-defectors-and-appointing.html>
6. <http://ddanchev.blogspot.com/2006/02/top-level-espionage-case-in-greece.html>
7. <http://ddanchev.blogspot.com/2006/07/indias-espionage-leaks.html>
8. <http://del.icio.us/DDanchev/Intelligence>
9. <http://del.icio.us/DDanchev/Espionage>

547

x

## **Luxury Vehicles on Demand (2006-10-12 15:02)**

[1]

Sharing luxury vehicles among club members who got bored of their Rolls Royce and want to experiment?

Propositions like these are rather common for NYC and Las Vegas where people do crazy things on the top of

their rich and bored euphoria – and why not?! Ultimate ownership as a driving force, or tiny private moment with



what you've always wanted, what would you chose?

*" Demand is increasing for alternatives to traditional ownership of high-end cars. Membership clubs and orga-*

*nizations offering fractional luxury-car ownership are in their infancy, as are agencies that rent new-model supercars, but they are expanding. More and more exotic-car drivers are finding they don't spend enough time in their cars to*

*justify owning them year-round and paying six-figure prices. If you're a Manhattan executive with a Lamborghini,*

*you probably don't drive it to work each day. You might only use it on vacation. Or maybe you only bring out your*

*Rolls-Royce. These are the kind of folks signing up. Another advantage of membership clubs is that instead of having to choose which car to buy, you can get a variety of different vehicles delivered in the course of a year. "It's a bit of an addictive thing," said Fuller. "Once you've driven a Ferrari and a Bentley and a Lamborghini and a Lotus, you ask,*

*'What's next on my hit list? '*

It's interesting to note that the major car manufacturers suffering from over-supply and becoming even more

insensitive to customers' preferences, are coming up with bargain deals when it comes to their most expensive

jewels.

Customer perceived pricing and value on luxury cars and brands positioned as the fastest, hottest, and trend-

setting vehicles, indeed play a crucial role in the profit margins here. Then again, building the ultimate beast and

waiting for a middle class citizen to finally manage to fulfil his or her America dream isn't really what liquidity is all about. Ownership of luxury vehicles though, is still very concentrated.

Intimate moment with your very own precious, or car manufacturers looking for greater liquidity while potentially turning luxury into a commodity?

A trend definitely worth keeping an eye on, just make sure you [2]join the club first.

1. [http://www.forbes.com/home/lifestyle/2006/09/29/ferrari-bentley-rolls-life-autos\\_cx\\_dl\\_1002carclubs.html](http://www.forbes.com/home/lifestyle/2006/09/29/ferrari-bentley-rolls-life-autos_cx_dl_1002carclubs.html)

2. <http://www.forbesautos.com/>

548



### **China Targeting U.S Satellite - Laser Ranging or Demonstration of Power? (2006-10-12 15:24)**

[1]

In previous posts "[2]Is a Space Warfare Arms Race Really Com-

ing?,"[3]Weaponizing Space and the Emerging Space Warfare Arms Race", and "[4]Anti-Satellite Weapons" I covered various developments and emerging trends in respect to space warfare. Last week, [5]China supposedly conducted a

jamming test on a U.S satellite, which is more of a [6]satellite ping in order to analyze the response data, rather than jamming :

*" The Defense Department remains tight-lipped about details, including which satellite was involved or when it*

*occurred. The Pentagon's National Reconnaissance Office Director Donald Kerr last week acknowledged the incident,*

*first reported by Defense News, but said it did not materially damage the U.S. satellite's ability to collect information.*

*"It makes us think," Kerr told reporters.*

*The issue looms large, given that U.S. military operations have rapidly grown more reliant on satellite data for*

*everything from targeting bombs to relaying communications to spying on enemy nations. Critical U.S. space assets*

*include a constellation of 30 Global Positioning Satellites that help target bombs and find enemy locations. This*

*system is also widely used in commercial applications, ranging from car navigation systems to automatic teller machines.*

*The Pentagon also depends on communications satellites that relay sensitive messages to battlefield comman-*

*ders, and satellites that track weather in critical areas so U.S. troops can plan their missions. "*

What this really was is a rather common [7]satellite ranging practice, thus determining the exact geocentric po-

sition of the U.S satellite and tracking it, which is a bit of a unethical move, but given there's no code of honor in

space yet, it's more of a demonstration of ongoing R &D activities to me.

1.

<http://photos1.blogger.com/blogger/1933/1779/1600/degnan3.jpg>

2. <http://ddanchev.blogspot.com/2006/03/is-space-warfare-arms-race-really.html>

3. <http://ddanchev.blogspot.com/2006/07/weaponizing-space-and-emerging-space.html>

4. <http://ddanchev.blogspot.com/2006/08/anti-satellite-weapons.html>

5.

[http://news.yahoo.com/s/nm/20061005/ts\\_nm/arms\\_space\\_dc](http://news.yahoo.com/s/nm/20061005/ts_nm/arms_space_dc)

6.

[http://www.ngs.noaa.gov/PUBS\\_LIB/Geodesy4Layman/TR80003D.HTM](http://www.ngs.noaa.gov/PUBS_LIB/Geodesy4Layman/TR80003D.HTM)

7. [http://en.wikipedia.org/wiki/Satellite\\_laser\\_ranging](http://en.wikipedia.org/wiki/Satellite_laser_ranging)



## **The History and Future of U.S. Military Satellite Communication Systems (2006-10-12 17:32)**

[1]

Resourceful and visually rich retrospective on the developments related to the

[2]U.S. Military Satellite Communication Systems :

*" Satellite communication has been a vital part of the United States military throughout the space age, begin-*

*ning in 1946, when the Army achieved radar contact with the moon. In 1954, the Navy began communications*

*experiments using the moon as a reflector, and by 1959, it had established an operational communication link*

*between Hawaii and Washington, D.C. As the U.S. space program grew in the 1960s, the Department of Defense*

*(DOD) began developing satellite communication systems that would address the special requirements of military*

*operations. In addition to protection against jamming, these needs included the flexibility to rapidly extend service to new regions of the globe and to reallocate system capacity as needed. "*

And here's what [3]the future – NCW all the way – has to offer  
:

*" Military satellite communications (or milsatcom) systems are typically categorized as wideband, protected, or narrowband. Wideband systems emphasize high capacity. Protected systems stress antijam features, covertness,*

*and nuclear survivability. Narrowband systems emphasize support to users who need voice or low-data-rate*

*communications and who also may be mobile or otherwise disadvantaged (because of limited terminal capability,*

*antenna size, environment, etc.). "*

Communications and PSYOPS win wars, information overload though, doesn't.

1.

<http://photos1.blogger.com/blogger2/4099/2257/1600/dorip03.0.png>

2.

<http://www.aero.org/publications/crosslink/winter2002/01.html>

3.

<http://www.aero.org/publications/crosslink/winter2002/08.html>

550

x

**North Korea's Nuclear Testing Roundup (2006-10-12 17:53)**

[1]

Way too much is happening right now, so here's are some of the articles, imagery and comments that made

me an impression recently. Go through [2]previous [3]coverage on [4]various [5]North Korean [6]developments in

case you're interested.

Anyway, [7]**Who needs nuclear weapons anymore?!**

## **Wikipedia**

[8]2006 North Korean nuclear test - full coverage, Wikipedia style

## **North Korea**

[9]Anti U.S Propaganda - 2004

[10]U.S. commits over 170 aerial espionage in May: DPRK

[11]U.S. Commits Over 180 Cases of Aerial Espionage against DPRK

[12]U.S. Imperialists Commit Aerial Espionage Against North Korea

[13]N Korea in 'US spy plane' warning

[14]North Korea's grisly arms tests on babies

[15]North Korea Condemns Japan for Militarization, Blames U.S. for Breakdown in Nuclear Talks

[16]Photos from Yongbyon nuclear site

[17]North Korea and Nuclear Weapons: The Declassified U.S. Record

## **Google Maps Imagery**

[18]North Korea Nuclear Test Site Eyeball

## **Commercial Satellite Imagery**

[19]The Nodong launch facility

[20]Possible Nuclear Test SiteP'unggye-yok, (Kilju / Kilchu / Kisshu / Gilju)

[21]Taepodong Missile Complex, North Korea – very good resolution!

## **Recent Developments Coverage**

[22]Nork Nuclear Test : It's a Dud (UPDATED)

[23]U.S "Dragnet" Hunts for Nuke Clues

[24]Korea Nuke : A 'Fizzle'?

[25]North Korea eases the heat on Iran - for now

[26]Iran does not criticize North Korea's nuclear test, blames Washington

[27]KGB had regularly told Russia on Pak-China-N-Korea nuke ties

[28]Pentagon Assesses Responses, Including a Possible Blockade

[29]U.S. opposed to raising S. Korea's surveillance alert: defense minister



[30]Diverted Attention, Neglect Set the Stage for Kim's Move

[31]Analysis: Should U.S. talk to N. Korea?

### **(Wrong) Speculations**

[32]CIA: North Korea Could Make 50 Nuclear Bombs a Year - 2002

[33]CIA says North Korea missile can reach U.S. - 2003

[34]North Korea's Nuclear Weapons: How Soon an Arsenal?

### **Interactives**

[35]North Korea Missile Range

551

[36]North Korea nuclear test picture gallery

[37]North Korea Nuclear Test photos

### **Russia**

[38]North Korea joins the nuclear club?

[39]Radiation in Russia normal after N. Korean nuclear test - agency

### **China**

[40]China opposes military action against N. Korea

[41]U.S. Congressman thanks China for informing U.S. of DPRK nuclear test

### **U.S**

[42]US missile defense said ready for N.Korea threat

[43]Responding to North Korea

[44]USA set to blockade North Korea and create defense complexes in space

[45]North Korean test 'went wrong,' U.S. official says

### **In-depth Analysis**

[46]North Korea Conducts Nuclear Test

1.  
[http://photos1.blogger.com/blogger2/4099/2257/1600/north\\_korea.jpg](http://photos1.blogger.com/blogger2/4099/2257/1600/north_korea.jpg)
2. <http://ddanchev.blogspot.com/2006/06/north-korea-turn-on-lights-please.html>
3. <http://ddanchev.blogspot.com/2006/07/north-koreas-cyber-warfare-unit-121.html>
4. <http://ddanchev.blogspot.com/2006/07/japans-reliance-on-us-spy-satellites.html>
5. <http://ddanchev.blogspot.com/2006/07/open-source-north-korean-imint.html>
6. <http://ddanchev.blogspot.com/2006/08/north-koreas-strategic-developments.html>
7. <http://ddanchev.blogspot.com/2006/02/who-needs-nuclear-weapons-anymore.html>
8.  
[http://en.wikipedia.org/wiki/2006\\_North\\_Korean\\_nuclear\\_test](http://en.wikipedia.org/wiki/2006_North_Korean_nuclear_test)

9. <http://www.kcna.co.jp/item/2004/200407/news07/26.htm>
10. [http://english.people.com.cn/200605/31/eng20060531\\_270083.html](http://english.people.com.cn/200605/31/eng20060531_270083.html)
11. [http://www1.korea-np.co.jp/pk/232th\\_issue/2006091404.htm](http://www1.korea-np.co.jp/pk/232th_issue/2006091404.htm)
12. [http://www.anti-imperialist.org/kcna-aerial-esp\\_9-1-03.html](http://www.anti-imperialist.org/kcna-aerial-esp_9-1-03.html)
13. <http://news.bbc.co.uk/2/hi/asia-pacific/5068662.stm>
14. [http://www.worldnetdaily.com/news/article.asp?ARTICLE\\_ID=50382](http://www.worldnetdaily.com/news/article.asp?ARTICLE_ID=50382)
15. <http://www.foxnews.com/story/0,2933,215863,00.html>
16. <http://www.isis-online.org/publications/dprk/photoindex.html>
17. <http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB87/>
18. <http://cryptome.org/dprk-test.htm>
19. <http://www.fas.org/nuke/guide/dprk/facility/nodong.htm>
20. <http://www.globalsecurity.org/wmd/world/dprk/kilju-punggye-yok.htm>
21. <http://www.satimagingcorp.com/gallery/north-korea-taepodong.html>
22. <http://www.defensetech.org/archives/002832.html>
23. <http://www.defensetech.org/archives/002833.html>

24. <http://www.defensetech.org/archives/002834.html>
25. [http://www.atimes.com/atimes/Middle\\_East/HJ11Ak01.html](http://www.atimes.com/atimes/Middle_East/HJ11Ak01.html)
26. [http://www.iht.com/articles/ap/2006/10/10/africa/ME\\_GEN\\_Ira\\_n\\_North\\_Korea.php](http://www.iht.com/articles/ap/2006/10/10/africa/ME_GEN_Ira_n_North_Korea.php)
27. <http://www.zeenews.com/znnew/articles.asp?aid=328438&sid=WOR>
28. [http://www.nytimes.com/2006/10/10/world/asia/10military.html?\\_r=1&oref=slogin](http://www.nytimes.com/2006/10/10/world/asia/10military.html?_r=1&oref=slogin)
29. [http://english.hani.co.kr/arti/english\\_edition/e\\_international/163073.html](http://english.hani.co.kr/arti/english_edition/e_international/163073.html)
30. [http://www.latimes.com/news/printedition/asection/la-fg-wrong10oct10,1,3420849.story?coll=la-news-a\\_secti552on&ctrack=1&cset=true](http://www.latimes.com/news/printedition/asection/la-fg-wrong10oct10,1,3420849.story?coll=la-news-a_secti552on&ctrack=1&cset=true)
31. [http://news.yahoo.com/s/ap/20061011/ap\\_on\\_go\\_pr\\_wh/talking\\_to\\_nkorea;\\_ylt=AtHQy0hGaFy0JjVQibjnQ9QD5gcF;\\_ylu=X3oDMTBjMHVqMTQ4BHNIYwN5bnN1YmNhda--](http://news.yahoo.com/s/ap/20061011/ap_on_go_pr_wh/talking_to_nkorea;_ylt=AtHQy0hGaFy0JjVQibjnQ9QD5gcF;_ylu=X3oDMTBjMHVqMTQ4BHNIYwN5bnN1YmNhda--)
32. <http://www.newsmax.com/archives/articles/2002/11/21/183623.shtml>

33. [http://www.ctv.ca/servlet/ArticleNews/story/CTVNews/1045074558238\\_42/?hub=CTVNewsAt11](http://www.ctv.ca/servlet/ArticleNews/story/CTVNews/1045074558238_42/?hub=CTVNewsAt11)
34. <http://www.fas.org/spp/starwars/crs/RS21391.pdf>
35. <http://www.cnn.com/interactive/world/0610/explainer.nkorea.missile/frameset.exclude.html?eref=yahoo>
36. <http://www.ft.com/cms/s/0584c88c-5846-11db-b70f-0000779e2340.html>
37. <http://en.rian.ru/photolents/20061009/54648750.html>
38. <http://en.rian.ru/analysis/20061010/54685965.html>
39. <http://en.rian.ru/russia/20061010/54676270.html>
40. [http://www.chinadaily.com.cn/china/2006-10/10/content\\_705284.htm](http://www.chinadaily.com.cn/china/2006-10/10/content_705284.htm)
41. [http://english.people.com.cn/200610/10/eng20061010\\_310408.html](http://english.people.com.cn/200610/10/eng20061010_310408.html)
42. [http://today.reuters.com/news/articleinvesting.aspx?view=CN&storyID=2006-10-09T203401Z\\_01\\_N09283080\\_RTRIDST\\_0\\_ARMS-LOCKHEED-KOREA.XML&rpc=66&type=qcna](http://today.reuters.com/news/articleinvesting.aspx?view=CN&storyID=2006-10-09T203401Z_01_N09283080_RTRIDST_0_ARMS-LOCKHEED-KOREA.XML&rpc=66&type=qcna)
43. <http://www.washingtonpost.com/wp-dyn/content/article/2006/10/09/AR2006100901137.html>
44. [http://english.pravda.ru/world/asia/10-10-2006/84970-Korea\\_explosion-0](http://english.pravda.ru/world/asia/10-10-2006/84970-Korea_explosion-0)

<http://edition.cnn.com/2006/WORLD/asiapcf/10/10/korea.nuclear.test/>

553



[1]

[2] Blogging for dollars is

ways of measuring their progress, or slowed down performance :

*realized that we needed to throw the net wider – this is where you come in! The working idea is to create a framework for measuring the ROI of external blogging efforts for medium- and large-sized companies. Below is an outline of*

*ingredients for the framework. Please help us by fleshing out sources, providing examples, and adding/editing our*

*ROI factors – feel free to add comments to this post or to [4] email us directly(if you'd prefer, we'll keep specific numbers and examples confidential and use them only as background). "*

What's my initial investment? It's time, and time doesn't really mean money, it means opportunities.

**My ROI factors :**

- visitors' retention
- blog stickiness
- average time spent
- echo-effect
- improved networking, communication with colleagues, friends, and of course, ordes of hypocrites
- successfully reaching, retaining, and informing predefined audiences
- differentiated content channel, barely links posting only
- third-party syndication
- self-preservation and self-awakening
- setting the foundation for my [5]successful identity upload and immortality into cyberspace?

Cloud courtesy of the main blog index and density of the keywords.

1.  
<http://photos1.blogger.com/blogger2/4099/2257/1600/MindStreams.jpg>
2.  
[http://money.cnn.com/magazines/business2/business2\\_archive/2006/09/01/8384325/](http://money.cnn.com/magazines/business2/business2_archive/2006/09/01/8384325/)
3.  
[http://blogs.forrester.com/charleneli/2006/10/calculating\\_the.html](http://blogs.forrester.com/charleneli/2006/10/calculating_the.html)
4. <mailto:cli@forrester.com,%20cstromberg@forrester.com?subject=ROI%20of%20blogging>
5.  
<http://www.blogcharm.com/Singularity/25603/Timetable.html>

554



## **Hunting the Hacker - Documentary (2006-10-14 20:14)**

[1]

Here's a recently released documentary – in Russian – entitled " **Охота на**

**хакера**", or Hunting the Hacker, discussing IT security, cyber crime, malware authors, online scams etc. It also features



[2]Eugene Kaspersky commenting on various trends. Don't forget, Russian hackers and Eastern European ones are

not just responsible for the sky-rocketing cyber-crime cost "projections", but for the global warming effect as well. I often come across biased comments on wrongly structured research questions such as : "Who are the best hackers

in respect to nationalities?", where it should have been formulated as "How vibrant is the IT security landscape, so that the changing dominance lifecycle of a nation could be measured at a particular moment in time?"

True hackers don't have nationalities, they're citizens of the world. [3]Download [4]or stream it from [5]Google

Video.

1.

[http://photos1.blogger.com/blogger2/4099/2257/1600/hunting\\_hacker.jpg](http://photos1.blogger.com/blogger2/4099/2257/1600/hunting_hacker.jpg)

2. [http://img152.imagevenue.com/img.php?](http://img152.imagevenue.com/img.php?image=19041_vlcsnap_207383_122_589lo.jpg)

[image=19041\\_vlcsnap\\_207383\\_122\\_589lo.jpg](http://img152.imagevenue.com/img.php?image=19041_vlcsnap_207383_122_589lo.jpg)

3.

[http://rapidshare.de/files/35918619/Oxota\\_na\\_xakra.part1.rar](http://rapidshare.de/files/35918619/Oxota_na_xakra.part1.rar)

4.

[http://rapidshare.de/files/35919839/Oxota\\_na\\_xakra.part2.rar](http://rapidshare.de/files/35919839/Oxota_na_xakra.part2.rar)

5. [http://video.google.com/videoplay?](http://video.google.com/videoplay?docid=7952991163803057724)  
[docid=7952991163803057724](http://video.google.com/videoplay?docid=7952991163803057724)

x

## North Korea's Wake-up Call (2006-10-15 00:26)

[1]

"Hey Dick, do you know what time it is? [2]It's Time to Bomb Kim Jong!"

1.

[http://photos1.blogger.com/blogger2/4099/2257/1600/wake\\_up\\_call.jpg](http://photos1.blogger.com/blogger2/4099/2257/1600/wake_up_call.jpg)

2. <http://www.youtube.com/watch?v=csnyiZx0Ho8>

556



## Observing and Analyzing Botnets (2006-10-16 01:15)

[1]

Informative and rich on visual materials, research presenting a "[2]A Multifaceted Approach to Understanding

the Botnet Phenomenon"

" Throughout a period of more than three months, we used this infrastructure to track **192 unique IRC botnets**

**of size ranging from a few hundred to several thousand infected end-hosts.** Our results show that botnets represent a major contributor to unwanted Internet traffic—27 % of all malicious connection attempts observed from our

distributed darknet can be directly attributed to botnetrelated spreading activity. Furthermore, **we**

***discovered***

***evidence of botnet infections in 11 % of the 800,000 DNS domains we examined***, indicating a high diversity among botnet victims. Taken as a whole, these results not only highlight the prominence of botnets, but also provide deep

*insights that may facilitate further research to curtail this phenomenon. "*

Botnets' security implications are often taken as a phenomenon, whereas this is not the case as distributed

computing concepts have been around for decades. Some interesting graphs and observations in this research are :

- Breakdown of scan-related commands seen on tracked botnets during the measurement period
- The percentage of bots that launched the respective services (AV/FW Killer) on the victim machines
- Distribution of exploited hosts extracted from the IRC tracker logs

**What botnet masters will definitely optimise :**

- disinformation for number and geolocation of infected hosts
- alternative and covert communication channels compared to stripped, or encrypted IRC sessions
- rethink of concept of performance vs stealthiness
- rethinking how to retain the infected nodes, compared to putting more efforts into infecting new ones

- for true competitiveness, vulnerabilities in anti-virus solutions allowing the code to remain undetected for as long as possible

- synchronization with results from popular test beds such as [3]VirusTotal for immediate reintroduction of an undetected payload

[4]The future of malware stands for solid ecosystem and [5]diversity, whereas, both, researchers, [6]the Pen-tagon, and malware authors are actively [7]benchmarking and optimising malware, each having seperate objectives to achieve.

Go through a previous post "[8]Malware Bot Families, Technology and Trends" in case you want to find out

more about botnet technologies, and update yourself with the most [9]recent case of DDoS extortion.

1. [http://photos1.blogger.com/blogger2/4099/2257/1600/Malicious\\_Pacman.jpg](http://photos1.blogger.com/blogger2/4099/2257/1600/Malicious_Pacman.jpg)
2. <http://www.cs.jhu.edu/~terzis/imc114f-aburajab.pdf>
3. <http://www.virustotal.com/>
4. <http://www.linuxsecurity.com/docs/malware-trends.pdf>

5. <http://ddanchev.blogspot.com/2006/09/malware-on-diebold-voting-machines.html>
6. <http://www.au.af.mil/au/awc/awcgate/afri/cybercraft.pdf>
7. <http://ddanchev.blogspot.com/2006/09/benchmarking-and-optimising-malware.html>
8. <http://ddanchev.blogspot.com/2006/08/malware-bot-families-technology-and.html>
9. [http://www.cio.com/blog\\_view.html?CID=25524](http://www.cio.com/blog_view.html?CID=25524)

557



## CIA's In-Q-Tel Investments Portfolio (2006-10-16 01:50)

[1]

In a previous post "[2]Aha, a Backdoor!" I discussed the "exemption" of publicly

traded companies from reporting to the SEC the usual way, and particularly their investments related to national

security. The strategy is visionary enough to act a major incentive factor for companies to both, [3]innovate, and

supply the [4]homeland security and defense markets.

However, [5]publicly obtainable data can still reveal historical developments:

*" A relatively unknown branch of the CIA is investing millions of taxpayer dollars in technology startups that, together, paint a map for the future of spying. Some of these technologies can pry into the personal lives of Americans not just for the government but for big businesses as well.*

*The CIA's venture capitalist arm, In-Q-Tel, has invested at least \$185 million in startups since 1999, molding*

*these companies' products into technologies the intelligence community can use.*

*More than 60 percent of In-Q-Tel's current investments are in companies that specialize in automatically col-*

*lecting, sifting through and understanding oceans of information, according to an analysis by the Medill School of*

*Journalism. While In-Q-Tel has successfully helped push data analysis technology ahead, implementing it within the*

*government for national security remains a challenge, and one of In-Q-Tel's former CEOs, Gilman Louie, has concerns*

*about whether privacy and civil liberties will be protected. "*

In a related Red Herring [6]article, In-Q-Tel points out that :

*"We don't just invest in equity of companies," said Scott Yancey, the firm's interim chief executive. "That's kind*

*of the hallmark of who we are in terms of being the strategic investor."*

*Observers said the payments don't fit with the typical venture model.*

*"To the extent that In-Q-Tel incentivizes its portfolio companies or employees otherwise, it sounds like from an*

*outsider's point of view that they've needed to create some artificial incentives that wouldn't otherwise be necessary in a traditional venture model," said Scott Joachim, a partner with the law firm Drinker, Biddle, & Reath."*

The Intelligence Community realizes that innovation will come from [7]outsiders working for insiders, and with

" more than 130 technology solutions to the intelligence community", CIA's In-Q-Tel seems to have made quite some

[8]sound investments.

A true angel investor in the "silent war". And yes, even you can [9]submit a business plan looking for seed

capital - and a "tail" to ensure you're developing in the right direction?

1. <http://photos1.blogger.com/blogger2/4099/2257/1600/in-q-tel-portfolio.jpg>

2. <http://ddanchev.blogspot.com/2006/05/aha-backdoor.html>

3. <http://news.moneycentral.msn.com/provider/providerarticle.asp?feed=AP&Date=20061005&ID=6081173>

4.

<http://www.signonsandiego.com/news/business/20060910-9999-1b10defense.html>

5.

[http://newsinitiative.org/story/2006/09/01/the\\_future\\_of\\_spying](http://newsinitiative.org/story/2006/09/01/the_future_of_spying)

6.

<http://www.redherring.com/Article.aspx?a=18351&hed=CIA+VC%E2%80%99s+Big+Spending>

7.

<http://f11.findlaw.com/news.findlaw.com/hdocs/docs/inqtel/inqtel80701rpt.pdf>

8.

<http://www.in-q-tel.com/invest/index.htm>

9.

<http://www.in-q-tel.com/submit/index.htm>

559

x

x

## **Registered Sex Offenders on MySpace (2006-10-17 00:00)**

[1]

Should you be [2]filtering online predators, prosecuting them, or monitoring their activities to analyze

and model the behaviour of the rest of them? Seems like [3]Kevin Poulsen's been data mining MySpace using the

[4]Department of Justice's National Sex Offender Register, and the results are a [5]Caught by Code MySpace Predator :



*" The automated script searched MySpace's 1 million-plus profiles for registered sex offenders - and soon found one that was back on the prowl for seriously underage boys.Excluding a handful of obvious fakes, I confirmed 744 sex*

*offenders with MySpace profiles, after an examination of about a third of the data. Of those, 497 are registered*

*for sex crimes against children. In this group, six of them are listed as repeat offenders, though Lubrano's previous convictions were not in the registry, so this number may be low. At least 243 of the 497 have convictions in 2000 or later. "*

[6]

These findings indicate the offenders' confidence in MySpace's inability to take the simplest measure -

match the publicly accessible data with its database - just in case. It's also worth mentioning that according to

a recently released [7]comScore analysis " *more than half of MySpace visitors are now age 35 or older*", and that according to their analysis, [8]Facebook, and [9]Xanga have much younger audiences, namely represent a top target

for online predators.

The most important issues however, remain the moment when a kid losses the communication with its "folks", and the huge amount of information kids share on any social networking site, thus unconsciously creating more contact points for the online predator.

[10]Internet Safety for Kids - a presentation for adults, is full with handy tips for educating and building aware-

ness on the problem.

1. [http://photos1.blogger.com/blogger2/4099/2257/1600/msoffenders3\\_f.jpg](http://photos1.blogger.com/blogger2/4099/2257/1600/msoffenders3_f.jpg)
2. <http://ddanchev.blogspot.com/2006/10/filtering-good-girls-and-im-threats.html>
3. <http://blog.wired.com/27bstroke6>
4. <http://www.nsopr.gov/>
5. <http://www.wired.com/news/technology/1,71948-0.html>
6. [http://photos1.blogger.com/blogger2/4099/2257/1600/social\\_network\\_demographics.jpg](http://photos1.blogger.com/blogger2/4099/2257/1600/social_network_demographics.jpg)
7. <http://www.comscore.com/press/release.asp?press=1019>
8. <http://www.facebook.com/>
9. <http://www.xanga.com/>
10. <http://www.packet-level.com/kids/handouts/iskhandout-20060111.pdf>

560

x

## **The Stereotyped Beauty Model (2006-10-18 20:39)**

[1]

If women/girls didn't hate each other so much, they could rule the world. [2]Nice ad counter-attacking the

entire "chickness ad model". Feels like Unilever got so successful promoting it, so that now they have to reposition themselves as a socially oriented company, not masters of Photoshop whose virtual creations [3]directly influence

McDonald's business model.

1.

[http://photos1.blogger.com/blogger2/4099/2257/1600/getting\\_hot.jpg](http://photos1.blogger.com/blogger2/4099/2257/1600/getting_hot.jpg)

2. <http://youtube.com/watch?v=knEIM16NuPg>

3. [http://www.dailymail.co.uk/pages/live/femail/article.html?in\\_article\\_id=406198&in\\_page\\_id=1879](http://www.dailymail.co.uk/pages/live/femail/article.html?in_article_id=406198&in_page_id=1879)

561

x

## **A Cost-Benefit Analysis of Cyber Terrorism (2006-10-18 21:01)**

[1]

What would the ROI be for a [2]terrorist organization wanting to take advantage of [3]cyberterrorism, and

how would they measure it?

Provocative perspective trying to emphasize on the minimal resources required to develop a cyberterrorism

platform, with very interesting assessments of various financial issues and possible casualties. "[4]A Cost-Benefit

Analysis of Cyber Terrorism" tries to answer:

*" Would cyberterrorism be a viable option for terrorists? This article addresses these questions assuming that*

*a hypothetical terrorist group, interested in adding cyberterrorism to its arsenal, de-cides to engage in a cost-benefit analysis to assess the payoffs and investment required by such a new endeavor. **The conclusions are that cy-***

***berterrorism is not a very efficient substitute for more traditional tools like bombs. It is more effective for the***

***terrorists to exploit information infrastructures to fight a "war of ideas," spreading their beliefs and points of view. "***

While the publication is released two years ago, it has recently come to the global attention that [5]Hezbollah

aren't exactly the type of cave-hiding individuals, ones fully realizing the concept of outsourcing instead of re-

inventing the wheel. While attacks on the [6]critical infrastructure, namely frontal cyberterrorism attacks are still

priority number one, and the [7]possible scenarios already tested numerous times, this "cyberterrorism myopia"

created many other dimensions of the concept.

**What went beneath the radar and consequently evolved?**

- online [8]radicalization, [9]propaganda, [10]communication, recruitment, education, and fund-raising actually

produce the "traditional terrorists"

- PSYOPS twisting the very foundations of the religion for the sake of a cause

- religious extremism started targeting more easily influenced/brainwashed youngsters while CCTVs were installed

on the hot spots, and new IDs when homegrown terrorists make the news

- [11]Hezbollah using U.S hosting companies since 1998

- [12]OSINT backed [13]PSYOPS improving the truthfulness of the statements

[14]Keep on reading and [15]data mining.

1.

<http://photos1.blogger.com/blogger2/4099/2257/1600/cbmatrix.gif>

2. <http://del.icio.us/DDanchev/Terrorism>

3. <http://del.icio.us/DDanchev/Cyberterrorism>

4.

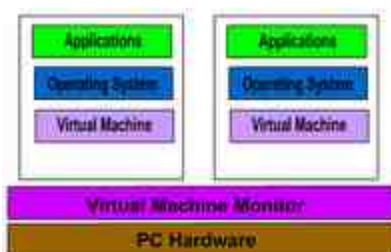
<https://www.webdepot.umontreal.ca/Usagers/langlost/MonDepotPublic/tic/cyber%20terror%20cost-benefit.pdf>

5.

[http://www.atimes.com/atimes/Middle\\_East/HI09Ak01.html](http://www.atimes.com/atimes/Middle_East/HI09Ak01.html)

6. <http://ddanchev.blogspot.com/2006/10/scada-security-incidents-and-critical.html>
7. <http://ddanchev.blogspot.com/2006/09/results-of-cyber-storm-exercise.html>
8. <http://ddanchev.blogspot.com/2006/06/tracking-down-internet-terrorist.html>
9. <http://www.haganah.org.il/haganah/index.html>
10. [http://ddanchev.blogspot.com/2006/08/cyber-terrorism-communications-and\\_22.html](http://ddanchev.blogspot.com/2006/08/cyber-terrorism-communications-and_22.html)
11. <http://www.haganah.org.il/harchives/005680.html>
12. <http://ddanchev.blogspot.com/2006/09/benefits-of-open-source-intelligence.html>
13. <http://ddanchev.blogspot.com/2006/09/internet-psyops-psychological.html>
14. <http://osint.blox.pl/>
15. [http://tajdeed-list.net/pipermail/pir\\_tajdeed-list.net/2006-June/000092.html](http://tajdeed-list.net/pipermail/pir_tajdeed-list.net/2006-June/000092.html)

562



Stand Alone Virtual Machine

## **Detecting Malware Time Bombs with Virtual Machines (2006-10-24 12:42)**

[1]

Back in June, details on an event that happened [2]during 2002 started emerging,

namely [3]UBS bank's employee use of a [4]logic bomb on the internal network that naturally had the type of insider empowerment it needed to spread :

*" According to prosecutors, shortly after Duronio created the code in late 2001, he quit his job and banked*

*thousands in "put" options against UBS, in which he would profit if the company's stock price declined by March 15, 2002, as a result of the attack he had allegedly set to launch against computer systems on March 4. Prosecutors*

*said that "within an hour or so" of walking out the door from UBS, Duronio was at a securities office buying "puts"*

*against UBS. The mail fraud charges relate to confirmation of purchases of the puts that were sent through the U.S.*

*Postal Service. The damage caused by the malicious code impaired trading at the firm that day, hampering more*

*than 1,000 servers and 17,000 individual work stations. The attack cost UBS about \$3 million to assess and repair,*

*said Assistant U.S. Attorney V. Grady O'Malley. "It took hundreds of people, thousands of man hours and millions of dollars to correct," O'Malley told jurors. "*

And while this isn't the last time logic bombs are used – [5]examples during the 80's – it's important to note

how flexible that type of malware could be, going way beyond the most common trigger - a [6]specific date and time.

The authors of "[7]Detecting Malware Timebombs with Virtual Machines" conducted research on automated

early warning system to shorten the time necessary to estimate the exact timetable of a malware in question :

*" Worms, viruses, and other malware can be ticking bombs counting down to a specific time, when they might,*

*for example, delete files or download new instructions from a public web server. We propose a novel virtual-machine-*

*based analysis technique to automatically discover the timetable of a piece of malware, or when events will be*

*triggered, so that other types of analysis can discern what those events are. This information can be invaluable for responding to rapid malware, and automating its discovery can provide more accurate information with less delay*

*than careful human analysis. "*

It successfully analyses Code Red, Klez, MyParty, Blaster, CME-24 and speculates on the future of the auto-

mated process. Worth reading and rethinking is the Internet's infected population actually the zombies, or aren't they the ones who still haven't been awakened?



1. <http://photos1.blogger.com/blogger2/4099/2257/1600/vm.gif>
2. <http://www.informationweek.com/news/showArticle.jhtml?articleID=189601826&subSection=Breaking+News>
3. [http://www.infoworld.com/article/06/06/08/79069\\_HNcomputerbomb\\_1.html](http://www.infoworld.com/article/06/06/08/79069_HNcomputerbomb_1.html)
4. <http://taosecurity.blogspot.com/2006/06/real-logic-bomb-logic-bomb-is-term.html>
5. <http://catless.ncl.ac.uk/Risks/5.63.html#subj1>
6. <http://ddanchev.blogspot.com/2006/02/cme-24-aka-nyxem-and-whos-infected.html>
7. <http://www.csif.cs.ucdavis.edu/~crandall/asplos06temporal.pdf>

563



**China's Information Security Market (2006-10-24 12:56)**

[1]

[2]China's information security market is very much into the introduction stage,

with perimeter based defenses acting as the main security solutions purchased there :

*" Statistics shows that the size of China information security market arrived at RMB 1080 million Yuan in Q2*

*2006, 21.35 % higher than the same period of last year, and 6.93 % more than Q1. In Q2 2006, sales revenue of*

*firewall products was RMB 474 million Yuan, and anti-virus software is RMB 305 million Yuan. Figure2 demonstrates*

*different security products market shares. Figure3 and Figure 4 list major vendors of firewall software and anti-virus software, respectively. "*

It's perhaps the perfect timing for you to find reliable channel partners and position yourself on the local mar-

ket that's about to attract even more government attention with the ongoing networking of China, thus a more

foreign-business-friendly security market than it is today. Among the most recent, and free of course, research on

the security market in China I often find myself coming back to is [3]Yan Liu's thesis on the current and future market

trends. From an investor's or analyst's point of view, you may also find [4]The Global State of Information Security in

2006 a very informative and rich on visual materials survey.

1.

<http://photos1.blogger.com/blogger2/4099/2257/1600/2006>

[829205356big2.jpg](#)

2.

<http://www.ccwresearch.com.cn/pubSystem/pubAdmin/switch.asp?ColumnId=1006&ArticleId=12221>

3. <http://www.dsv.su.se/research/seclab/pages/pdf-files/2006-x-362.pdf>

4. [http://www.cio.com/archive/091506/security\\_survey.html](http://www.cio.com/archive/091506/security_survey.html)

564



## **The Surveillance System About to Get Overloaded (2006-10-24 14:19)**

[1]

I wonder would they later on publicly announce "Hall of Fame/Shame" of the

most regular drinkers, and actually use to data to fuel growth in local anti-drinking initiatives based on the most

"affected" regions? [2] Beer fingerprints to go UK-wide :

*" The government is funding the roll out of fingerprint security at the doors of pubs and clubs in major English cities. Funding is being offered to councils that want to have their pubs keep a regional black list of known trouble*

*makers. The fingerprint network installed in February by South Somerset District Council in Yeovil drinking holes is being used as the showcase. "*

Use a public WC - [3]Big Brother's peeping, have a beer - it's on Big Brother's bill, and if this isn't a total abuse of technology and tax payer's money to spy on them, what is? A system like this would be useless to local bartenders, to

be honest their experience for spotting the drunken monkeys or knowing them would prove invaluable in this case.

From another perspective, these trouble makers, given they don't trash the place, are actually among the major consumers there.

The article makes a good point through - if pubs and clubs get extra monitoring, domestic violence increases,

so would you install CCTVs at home to prevent it through the "psychological effect" as well?

1. <http://photos1.blogger.com/blogger2/4099/2257/1600/heineken.jpg>

2. [http://www.theregister.co.uk/2006/10/20/pub\\_fingerprints/](http://www.theregister.co.uk/2006/10/20/pub_fingerprints/)

3. <http://ddanchev.blogspot.com/2006/06/big-brother-in-restroom.html>

## **What are you Looking at? (2006-10-26 15:13)**

[1]

You piece of EyeBall surveillance camera!

1.

<http://photos1.blogger.com/blogger2/4099/2257/1600/Shot0001.jpg>

566



## **Ms. Dewey on Microsoft and Security (2006-10-26 15:31)**

[1]

She sure knows "[2]all these little ones and zeroes", and your [3]social security number

altogether. I like the idea, reminds of the futuristic holograms of Einstein acting as interactive Wikipedia which when

asked about WWII starts projecting battles – she's thinking way too long, but as she pointed out she's just a chick in

front of your computer.

1.

<http://photos1.blogger.com/blogger2/4099/2257/1600/dewey.jpg>

2. <http://www.msdevey.com/index.html?s=microsoft&r=CO-007>

3. <http://www.msdevey.com/index.html?s=security&r=SC-013>

567



## **ShotSpotter - Gunshot Sensors Network (2006-10-26 15:55)**

[1]

[2]ShotSpotter is :

*" a network of noise sensors that identifies and pinpoints gunfire. Over the past few weeks, the technology has guided police to three homicides in Southeast Washington, and in one case officers got there rapidly enough to make an arrest.*

*ShotSpotter complements 48 surveillance cameras installed in many city neighborhoods.*

*But unlike the cam-*

*eras, which are checked after the fact, ShotSpotter gets word to police as soon as bullets start flying – in many cases before anyone has a chance to call 911. Over the past two months, the sensors, roughly the size of coffee cans, have been hidden atop buildings in many sections of Southeast Washington. "*

[3]Innovative, but how well is it performing when it comes to filtering a three cars synchronized gangsta rap

music, and the not so fashionable, but adaptive use of [4]silencers? It makes me think on the possibility of disinfor-

mation by criminals knowing someone's listening and responding to gunshots. On the other hand, it could have ever

wider acceptance in a war zone acting as an early warning system.

**UPDATE:** [5]Techdirt's comments on the system.

1. <http://photos1.blogger.com/blogger2/4099/2257/1600/p5864.0.jpg>

2. <http://www.shotspotter.com/>

3. <http://www.washingtonpost.com/wp-dyn/content/article/2006/10/21/AR2006102100826.html>

4. <http://en.wikipedia.org/wiki/Suppressor>

5. <http://www.techdirt.com/articles/20061026/090955.shtml>



## Real-Time Spam Outbreak Statistics (2006-10-28 20:57)

[1]

Following my previous posts on "[2]Real-Time PC Zombie Statistics", and

"[3]Email Spam Harvesting Statistics", you may also find WatchGuard's recently [4]released real-time spam outbreak statistics entertaining :

*" Once in a while as I'm getting flooded with some particularly repititious spam bomb, I wonder whether other networks are receiving the same dumb stuff. And occasionally, I wonder where it originated from.*

*Both questions are readily answered with a [5] nifty Web utilityprovided by the CommTouch Detection Center.*

*[Full disclosure: WatchGuard's spamBlocker product is powered by a license with CommTouch.] The utility shows*

*a map of the world, with red spots indicating the approximate location of new spam outbreaks. If you hover your*

*cursor over any of the red zones, a popup box shows the subject lines of the most recently detected spam. It's an*



*easy, instant way to verify whether an email you received is part of a spampaign. "*

Naturally, the stats are only limited to the vendor's sensor network worldwide, whereas you still get the chance to

feel the dynamics of spam outbreaks worldwide. I often speculate – and got the case studies proving it – that the

more pressure is put on [6]spammers, [7]phishers and [8]malware authors, the higher would their consolidation

become. For the time being, spammers are mostly utilizing the cost-effective one-to-many communication model,

and their ROI – where the investment is in renting infected zombie PCs – is positive by default without them even

segmenting, targeting and actually reaching the most gullible audience. If spammers change this model, it would

mean a much faster email services worldwide, but for the time being, number of messages sent compared to basic

marketing practices seems to be the benchmark.

Spammers got the "contact points", malware authors the platform and the payload, and phishers the social

engineering "know-how", I find spammers missing so badly these days – the trade off for delivering the spam through content obfuscation is the quality of the message itself.

Trouble is, they'll soon realize that marriage is better than

the divorce and unite forces given the pressure.

**UPDATE:** "[9]Bot nets likely behind jump in spam" discusses the consolidation, or the possibility for services on

demand. Via [10]Sunbelt's blog.

1. [http://photos1.blogger.com/blogger2/4099/2257/1600/real\\_time\\_spam\\_outbreak.jpg](http://photos1.blogger.com/blogger2/4099/2257/1600/real_time_spam_outbreak.jpg)
2. <http://ddanchev.blogspot.com/2006/06/real-time-pc-zombie-statistics.html>
3. <http://ddanchev.blogspot.com/2006/09/email-spam-harvesting-statistics.html>
4. <http://www.watchguard.com/products/realtime-monitor.asp>
5. <http://www.watchguard.com/products/realtime-monitor.asp>
6. <http://ddanchev.blogspot.com/2006/06/over-performing-spammer.html>
7. <http://ddanchev.blogspot.com/2006/09/google-anti-phishing-black-and-white.html>
8. <http://ddanchev.blogspot.com/2006/09/benchmarking-and-optimising-malware.html>
9. <http://www.securityfocus.com/news/11420>
10. <http://sunbeltblog.blogspot.com/2006/10/spam-yeah-its-up.html>

569

x

## **Face Recognition on 3G Cell Phones (2006-10-29 00:41)**

[1]

[2]Face recognition isn't just done at home courtesy of MyHeritage.com, but on-the-go with yet another

[3]release of face recognition authentication for cell phones by a leading mobile operator in Japan :

*" Security features include biometric authentication (user's face) and compatibility with DoCoMo's Omakase Lock™*

*remote locking service, as well as the Data Security Service™ for backing up phonebooks and other important data*

*on a network server. The model can function as an e-wallet, timecard and personal identification card for accessing*

*restricted areas. "*

The concept has been around for quite some time, but with Japan representing one of the most [4]mature markets for

mobile devices – right after South Korea – the feature would briefly gain popularity and acceptance. The interesting

part is the [5]security vs usability issue as if the face recognition doesn't provide perfect results in every environment and under external factors such as darkness or even brightness, by the time the technology matures, a secret question

to further authenticate or good old PIN code would do the work.

Here's a [6]very well sorted library of various research on the topic, and an interesting service that's [7]sharing a stolen phone's photos.

1. <http://photos1.blogger.com/blogger2/4099/2257/1600/docomo.0.jpg>
2. <http://ddanchev.blogspot.com/2006/08/face-recognition-at-home.html>
3. <http://www.nttdocomo.com/pr/2006/001293.html>
4. <http://planetinternet.wordpress.com/2006/04/19/lessons-from-3g-in-japan-and-south-korea/>
5. [http://www.usatoday.com/tech/news/techinnovations/2003-11-14-location\\_x.htm](http://www.usatoday.com/tech/news/techinnovations/2003-11-14-location_x.htm)
6. <http://www.face-rec.org/interesting-papers/>
7. <http://slashdot.org/articles/06/09/01/2334239.shtml>

570



## **Greetings Professor Falken (2006-10-29 01:43)**

[1]

The [2]classic that originally started the war dialing generation seems to never

fade, and its core idea of simulating a Global Thermonuclear War has motivated [3]the authors of [4]Defcon - The

Game to come up with a fully realistic representation of it. I recently took the time to play around with it - it's so

compact you can even play it on a removable media -, and I must say I never enjoyed seeing my missile projections

and the sound effects out of my launches. [5]The trailer speaks for itself!

Rule number one of thermonuclear war, launch your ICBMs as soon as you hear the Defcon 1 alert, or you risk losing

your silos due to the AIs "shooting into the dark" or conducting reconnaissance, however, keep one silo - each has 10 ICBMs reaching anywhere on the map - as you wouldn't be able to hit the biggest cities by the time you don't

neutralize the surrounding air-defense. Submarines are sneaky and very powerful with each holding 5 missiles, but

firing occurs if the target is within range so make sure you position yourself where you should be. Sea and air-to-air

battles are very common and there aren't any land conflicts at all. Make sure you don't fire from numerous submarines

simultaneously, as if there's a fighter in the air it will detect and attack the submarine. On the other hand, use fighters to distract the air-defense firing at them while your ICBMs pass through and reach their target. If I were to describe

the WarGames simulation in two words, that would be, tense and very addictive. Moreover, you don't need a multi-

million game or movie budget to make an impression, as this game, and "[6]The Day After" do. Goodbye Europe -

alliances are a powerful force given you convince some Als to ally with you, but at the end there could be only one

winner.

1.

<http://photos1.blogger.com/blogger2/4099/2257/1600/defcon.jpg>

2. <http://ddanchev.blogspot.com/2006/03/dvd-of-weekend-war-games.html>

3. <http://www.introversion.co.uk/defcon/>

4. [http://en.wikipedia.org/wiki/DEFCON\\_\(computer\\_game\)](http://en.wikipedia.org/wiki/DEFCON_(computer_game)).

5. <http://www.introversion.co.uk/defcon/videos/trailer1.wmv>

6. <http://www.imdb.com/title/tt0085404/>

571



The screenshot shows a web form titled "Fake Search Warrant Generator". It contains several input fields for personal information: Name, Address, City, State, Zip, and Phone. There are also checkboxes for "I am a resident of the United States" and "I am a citizen of the United States". A section for "Description of the search" is present, with a text area for details and a dropdown menu for "Type of search". At the bottom, there is a "Generate" button and a "Print" button. The form is designed to look like a legal document, with a header section for "Case Information" and a footer section for "Judge Information".

## Fake Search Warrant Generator (2006-10-30 17:40)

[1]

In response to [2]Christopher Soghoian's home raid - the [3]masked superhero

by night – a [4]fake search warrant generator was just released :

*" for district courts all across the United States with the intent of improving national security by reducing the amount of time it takes for our public guardians to create search warrants. "*

Sarcasm's most effective when having a point.

1. [http://photos1.blogger.com/blogger2/4099/2257/1600/search\\_warrant\\_generator.jpg](http://photos1.blogger.com/blogger2/4099/2257/1600/search_warrant_generator.jpg)
2. <http://www.securityfocus.com/brief/342>
3. <http://slightparanoia.blogspot.com/>
4. <http://www.dehp.net/fakewarrant/>

572

## **2.11 November**

573

x

## **Proof of Concept Symbian Malware Courtesy of the Academic World (2006-11-01 19:03)**

[1]

Know your enemy to better predict his moves and future strategies as Symbian [2]malware optimization is

getting the necessary attention from the academic community :

*" The University of Santa Barbara's software group released the [3] source code for their proof of concept 'Feakk' worm that was developed by Paul Haas in March 2005. The worm uses SMS to send a hyperlink to its target. The targeted*

*user then has to visit the hyperlink and download and acknowledge three sets of prompts in order for the worm to*

*install, at which point it will immediately start to run in the background. It will scan the user's contact list and send a message to each contact (including the recipients' names) and will also scan for new contacts at certain intervals.*

*Upon installation, the worm checks for a contact with the first name "HACKME." If this isn't found the worm will exit. If it is found, then the worm sends itself to every mobile number it finds in the user's contact list. The author did not write a payload because this was for demonstration purposes only and it should be noted that it can be*

*removed via the "Uninstall List. "*

While malware authors will turn the concept into a commodity, it doesn't exploit a specific OS vulnerability,

thus the possibility of large scale outbreaks doesn't really exist at all. In a [4]previous post I commented on some

future developments related to the penetration of mobile devices in our daily lives and the trust factor assuming

whoever holds the handset is actually the one using it :

*" Malware authors indeed have [5] financial incentives to further continue recompiling publicly available PoC mobile malware source code, and it's the purchasing/identification features phones, opening a car with an SMS, opening a door*



*with an SMS, purchasing over an SMS or direct barcode scanning, mobile impersonation scams, harvesting*

*phone numbers of infected victims, as well as unknowingly interacting with premium numbers are the things about*

*to get directly abused - efficiently and automatically. "*

Digitally fingerprinting mobile malware may be marketable, but it's [6]rather useless as we've seen in the past

compared to basic user awareness.

I feel the [7]University of Santa Barbara's software group are very much on the right track, conducting research on

OS and application specific vulnerabilities, as they've released quite some interesting papers during 2006 :

[8]Advanced Attacks Against PocketPC Phones

[9]PocketPC MMS - Remote Code Injection/Execution Vulnerability and Denial-of-Service

[10]Vulnerability Analysis of MMS User Agents

[11]Security of Smart Phones

[12]Using Labeling to Prevent Cross-Service Attacks Against Smart Phones

1.

[http://www.symantec.com/enterprise/security\\_response/weblog/2006/10/university\\_of\\_santa\\_barbara\\_re.html](http://www.symantec.com/enterprise/security_response/weblog/2006/10/university_of_santa_barbara_re.html)

2. <http://ddanchev.blogspot.com/2006/09/benchmarking-and-optimising-malware.html>

3. <http://www.cs.ucsb.edu/~rsg/projects/smartphones/cell.zip>
4. [http://ddanchev.blogspot.com/2006/08/bed-time-reading-symbian-os-platform\\_12.html](http://ddanchev.blogspot.com/2006/08/bed-time-reading-symbian-os-platform_12.html)
5. <http://www.symantec.com/avcenter/venc/data/trojan.redbrowser.a.html>
6. <http://www.securityfocus.com/news/11379>
7. <http://www.cs.ucsb.edu/~rsg/projects/smartphones/>
8. [http://www.cs.ucsb.edu/~rsg/projects/smartphones/2006\\_mulliner\\_DEFCON\\_slides.pdf](http://www.cs.ucsb.edu/~rsg/projects/smartphones/2006_mulliner_DEFCON_slides.pdf)
9. [http://www.cs.ucsb.edu/~rsg/projects/smartphones/mms\\_advisory.txt](http://www.cs.ucsb.edu/~rsg/projects/smartphones/mms_advisory.txt)
10. [http://www.cs.ucsb.edu/~rsg/projects/smartphones/2006\\_mulliner\\_vigna\\_ACSAC.pdf](http://www.cs.ucsb.edu/~rsg/projects/smartphones/2006_mulliner_vigna_ACSAC.pdf)
11. [http://www.cs.ucsb.edu/~rsg/projects/smartphones/2006\\_mulliner\\_MSThesis.pdf](http://www.cs.ucsb.edu/~rsg/projects/smartphones/2006_mulliner_MSThesis.pdf)
12. [http://www.cs.ucsb.edu/~rsg/projects/smartphones/2006\\_mulliner\\_vigna\\_dagon\\_lee\\_DIMVA.pdf](http://www.cs.ucsb.edu/~rsg/projects/smartphones/2006_mulliner_vigna_dagon_lee_DIMVA.pdf)

574

575

## FAS's Immune Attack Game (2006-11-01 20:09)

[1]

[2]Professor Falken would have loved this one. The Federation of American Scientists recently released their

[3]report from the [4]Summit on Educational Games, and an upcoming educational game :

" *Immune Attack is a first person strategy PC video game that teaches immunological principles through entertaining game play. **The protagonist, a teenaged prodigy with a unique condition in which the immune system is "present,***

***yet non-functional", must pilot a microscopic nanobot to save his own life.*** He must teach his semi-functional immune system to fight off diseases and bacterial/viral infections by programming individual cell types. This programming is accomplished through the successful completion of various educational minigames, each of which teach a central

*immunology principle and, once completed, confer added ability to the selected cell type. "*

Here're two more reports you may find informative on [5]the future of learning [6]through games – the [7]game

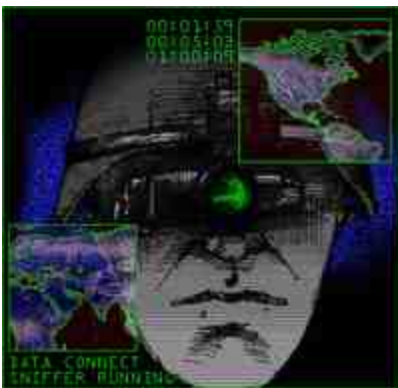
addicts still got a chance.

1.

<http://photos1.blogger.com/blogger2/4099/2257/1600/MacrophageBacteria.0.jpg>

2. <http://ddanchev.blogspot.com/2006/10/greetings-professor-falken.html>
3. <http://fas.org/gamesummit/Resources/Summit%20on%20Educational%20Games.pdf>
4. <http://fas.org/gamesummit/>
5. <http://www.cra.org/reports/cyberinfrastructure.pdf>
6. <http://www.academiccolab.org/resources/gappspaper1.pdf>
7. [http://www.yikers.com/video\\_kids\\_addiction\\_to\\_world\\_of\\_warcraft\\_ruins\\_his\\_familys\\_life.html](http://www.yikers.com/video_kids_addiction_to_world_of_warcraft_ruins_his_familys_life.html)

576



**Delicious Information Warfare - Friday (2006-11-03 04:04)**

[1]

Wish I could blog everything I read and makes me [2]an impression but that's

not the point. The point is to emphasize on the big picture, and find the balance between information overload and information underload.

**01. [3]North Korea, Turkmenistan, Eritrea the worst violators of press freedom** - Journalists in North Korea, Eritrea, Turkmenistan, Cuba, Burma and China are still risking their life or imprisonment for trying to keep us

informed. **to [4]FreeSpeech [5]Censorship**

**02. [6]When North Korea Falls** - The furor over Kim Jong Il's missile tests and nuclear brinksmanship obscures the real threat: the prospect of North Korea's catastrophic collapse. How the regime ends could determine the

balance of power in Asia for decades. The likely winner? China **to [7]Geopolitics**

**03. [8]U.S. revives terror data mining** - In response to concerns about the program's privacy and civil liberties implications, Congress in 2003 cut all funding for it, but research continued in different agencies, funded by classified appropriations for Pentagon intelligence agencies. **to [9]Intelligence [10]Terrorism**

**04.**

**[11]Singapore Slings Censorship** - StarHub Cable Vision of Singapore is being fined \$6,350 for showing

footage of lesbian sex and bondage during episodes of the reality program "Cheaters." **to [12]Censorship [13]Singapore**

**05. [14]Googlers Worldwide -** Number of Google employees 2004-2006. **to [15]Google**

**06. [16]Can IPS Alleviate The Botnet Problem? -** Next-Generation IPS devices bring a number of extra bene-

fits, and solve many of the botnet problems. When deployed at the network edge, IPS devices can see all traffic

entering and exiting the network. **to [17]Security [18]Malware [19]Botnet [20]IPS**

**07. [21]Abu Ghraib Photos, Videos To Come -** The ACLU has sought the release of 87 photos and four video-

tapes taken at the prison as part of an October 2003 lawsuit demanding information on the treatment of detainees

in U.S. custody and the transfer of prisoners to countries known to use torture. **to [22]Military [23]PSYOPS**

**08. [24]'Censorship' controversy? Sometimes it's just part of the ad campaign -** NBC and the CW network

had refused to run ads in which the singer Natalie Maines refers to President George W. Bush with an expletive and

as "dumb." **to [25]Censorship [26]Advertising**

**09.**

**[27]Rutkowska: Anti-Virus Software Is Ineffective -** Stealth malware researcher Joanna Rutkowska dis-

cusses her interest in computer security, the threat from rootkits and why the world is not ready for virtual machine

technology. **to [28]Malware [29]Interview**

**10. [30]Under Fire, Soldiers Kill Blogs** - Some of the web's more popular "milblogs" – blogs maintained by present or former active duty military personnel – are going quiet following a renewed push by U.S. military officials

to scan sites for security risks. **to [31]Blog [32]Military [33]OPSEC**

**11. [34]Is Google Evil?** - Internet privacy? Google already knows more about you than the National Security Agency ever will. **to [35]Google [36]Privacy**

**12. [37]Google Earth Update of Eyeballs 1 - ECHELON's Global Stations** - Sebana Seca Echelon Station, Pine

Gap Echelon Station, Geraldton Echelon Station, Misawa Echelon Station, Kunia Echelon Station, Waihopai Echelon

Station. **to [38]OSINT [39]ECHELON [40]Intelligence [41]SIGINT**

**13. [42]U.N. blasts Cisco, others on China cooperation** - "It's the same equipment that we sell in every country around the world in which we sell equipment," said Art Reilly, Cisco's senior director for strategic technology policy. "There is no differentiation." **to [43]Censorship [44]China [45]Microsoft [46]Google [47]Yahoo [48]Cisco 14.**

**[49]GAO: Better coordination of cybersecurity R & D needed** - DOD officials told GAO that the depart-

ment provided about \$150 million to its cybersecurity research programs in fiscal 2005. **to [50]Security**

**15. [51]The Reinvention Of Martha Stewart** - Stewart no longer has total control over the brand she built.

She still owns the bulk of the company's stock and holds 92 % of the voting power-prompting speculation that she may one day take it private-but she can't dictate the agenda. **to [52]Branding**

**16.**

**[53]Raytheon Announces Revolutionary New 'Cockpit' For Unmanned Aircraft** - "We took the best-of-

breed technologies from the gaming industry and coupled them with 35-years Raytheon UAS command and control

expertise and developed a state-of-the-art universal cockpit built around the operator". **to [54]Military [55]UAV**

**17. [56]The Tangram Intelligence Program** - The Tangram program makes no distinction between intentional

and deliberate acts to avoid detection versus the consequences of spotty collection and reporting of intelligence. **to**

**[57]Intelligence [58]TIA [59]Tangram**

**18. [60]Intellipedia - a Classified Wiki** - Intellipedia is a classified wiki that runs on JWICS, the top-secret network Intelink that links the 16 agencies that comprise the U.S. intelligence community. It is not accessible to the

public. **to [61]Intelligence [62]Wikipedia**

**19. [63]China: We don't censor the Internet. Really** - We have hundreds of journalists in China, and some



of them have legal problems. It has nothing to do with freedom of expression. **to** [64]**Censorship** [65]**China**

[66]**FreeSpeech**

**20. [67]Ratings Table of EU and Leading Surveillance Societies** - This year Privacy International took the decision to use the report as the basis for a ranking assessment of the state of privacy in all EU countries together with

eleven benchmark countries. **to** [68]**Privacy** [69]**Surveillance** [70]**1984**

**21. [71]Watch a live spam bot in action** - Take a peek with me into one trojan's junkmail activities. The following account is happening as I type, and shows that some image spam is not unique even though it appears to be

random. **to** [72]**Malware** [73]**Bots** [74]**Spam**

**22. [75]OS X proof of concept virus -Macarena** - OSX.Macarena is a proof of concept virus that infects files in the current folder on the compromised computer. **to** [76]**Malware** [77]**MAC**

**23. [78]American Leadership and War** - Which presidents and political parties were responsible for America's 578

deadliest wars? Republicans, Democrats, or the Founding Fathers? This map answers our question by illustrating the history of American conflict from the Revolutionary War to Iraq. **to** [79]**Military** [80]**War** [81]**Leadership** **24. [82]Diebold slams HBO Hacking Democracy documentary** - According to Diebold, 40 per cent of votes

this November will be recorded electronically with its own machines accounting for 40 per cent of that market. **to**

[83]**Security** [84]**Diebold** [85]**Voting**

1. [http://photos1.blogger.com/blogger2/4099/2257/1600/infowar\\_soldier.gif](http://photos1.blogger.com/blogger2/4099/2257/1600/infowar_soldier.gif)
2. <http://del.icio.us/DDanchev>
3. [http://www.rsf.org/rubrique.php3?id\\_rubrique=639](http://www.rsf.org/rubrique.php3?id_rubrique=639)
4. <http://del.icio.us/DDanchev/FreeSpeech>
5. <http://del.icio.us/DDanchev/Censorship>
6. <http://www.theatlantic.com/doc/200610/kaplan-korea>
7. <http://del.icio.us/DDanchev/Geopolitics>
8. <http://washingtontimes.com/national/20061025-102921-8851r.htm>
9. <http://del.icio.us/DDanchev/Intelligence>
10. <http://del.icio.us/DDanchev/Terrorism>
11. [http://blog.washingtonpost.com/offbeat/2006/10/singapore\\_slings\\_censorship.html](http://blog.washingtonpost.com/offbeat/2006/10/singapore_slings_censorship.html)
12. <http://del.icio.us/DDanchev/Censorship>
13. <http://del.icio.us/DDanchev/Singapore>
14. <http://www.zorgloob.com/images/googlersgraph.jpg>

15. <http://del.icio.us/DDanchev/Google>
16. <http://www.securitypronews.com/news/securitynews/spn-45-20061026CanIPSAleviatetheBotnetProblem.html>
17. <http://del.icio.us/DDanchev/Security>
18. <http://del.icio.us/DDanchev/Malware>
19. <http://del.icio.us/DDanchev/Botnet>
20. <http://del.icio.us/DDanchev/IPS>
21. [http://www.jihadunspun.com/intheatre\\_internal.php?article=106633&list=/home.php](http://www.jihadunspun.com/intheatre_internal.php?article=106633&list=/home.php)
22. <http://del.icio.us/DDanchev/Military>
23. <http://del.icio.us/DDanchev/PSYOPS>
24. <http://www.iht.com/articles/2006/10/29/business/film.php>
25. <http://del.icio.us/DDanchev/Censorship>
26. <http://del.icio.us/DDanchev/Advertising>
27. <http://www.eweek.com/article2/0,1759,2040760,00.asp?kc=EWRSS03129TX1K0000614>
28. <http://del.icio.us/DDanchev/Malware>
29. <http://del.icio.us/DDanchev/Interview>
30. <http://wired.com/news/politics/0,72026-0.html>
31. <http://del.icio.us/DDanchev/Blog>

32. <http://del.icio.us/DDanchev/Military>
33. <http://del.icio.us/DDanchev/OPSEC>
34. <http://www.motherjones.com/news/feature/2006/11/google.html>
35. <http://del.icio.us/DDanchev/Google>
36. <http://del.icio.us/DDanchev/Privacy>
37. <http://cryptome.org/google/google-update1.htm>
38. <http://del.icio.us/DDanchev/OSINT>
39. <http://del.icio.us/DDanchev/ECHELON>
40. <http://del.icio.us/DDanchev/Intelligence>
41. <http://del.icio.us/DDanchev/SIGINT>
42. [http://news.com.com/2100-1028\\_3-6131010.html](http://news.com.com/2100-1028_3-6131010.html)
43. <http://del.icio.us/DDanchev/Censorship>
- 579
44. <http://del.icio.us/DDanchev/China>
45. <http://del.icio.us/DDanchev/Microsoft>
46. <http://del.icio.us/DDanchev/Google>
47. <http://del.icio.us/DDanchev/Yahoo>
48. <http://del.icio.us/DDanchev/Cisco>
49. [http://www.gcn.com/online/vol1\\_no1/42465-1.html](http://www.gcn.com/online/vol1_no1/42465-1.html)

50. <http://del.icio.us/DDanchev/Security>
51. [http://www.businessweek.com/magazine/content/06\\_45/b4008076.htm](http://www.businessweek.com/magazine/content/06_45/b4008076.htm)
52. <http://del.icio.us/DDanchev/Branding>
53. [http://www.spacewar.com/reports/Raytheon\\_Announces\\_Revolutionary\\_New\\_Cockpit\\_For\\_Unmanned\\_Aircraft\\_999.html](http://www.spacewar.com/reports/Raytheon_Announces_Revolutionary_New_Cockpit_For_Unmanned_Aircraft_999.html)
54. <http://del.icio.us/DDanchev/Military>
55. <http://del.icio.us/DDanchev/UAV>
56. <http://www.cryptome.org/tangram-intel.htm>
57. <http://del.icio.us/DDanchev/Intelligence>
58. <http://del.icio.us/DDanchev/TIA>
59. <http://del.icio.us/DDanchev/Tangram>
60. <http://en.wikipedia.org/wiki/Intellipedia>
61. <http://del.icio.us/DDanchev/Intelligence>
62. <http://del.icio.us/DDanchev/Wikipedia>
63. [http://news.com.com/China+We+dont+censor+the+Internet.+Really/2100-1028\\_3-6130970.html](http://news.com.com/China+We+dont+censor+the+Internet.+Really/2100-1028_3-6130970.html)
64. <http://del.icio.us/DDanchev/Censorship>

65. <http://del.icio.us/DDanchev/China>
66. <http://del.icio.us/DDanchev/FreeSpeech>
67. <http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-545223>
68. <http://del.icio.us/DDanchev/Privacy>
69. <http://del.icio.us/DDanchev/Surveillance>
70. <http://del.icio.us/DDanchev/1984>
71. <http://www.avertlabs.com/research/blog/?p=123>
72. <http://del.icio.us/DDanchev/Malware>
73. <http://del.icio.us/DDanchev/Bots>
74. <http://del.icio.us/DDanchev/Spam>
75. [http://www.symantec.com/enterprise/security\\_response/writ eup.jsp?docid=2006-110217-1331-99&tabid=1](http://www.symantec.com/enterprise/security_response/writ eup.jsp?docid=2006-110217-1331-99&tabid=1)
76. <http://del.icio.us/DDanchev/Malware>
77. <http://del.icio.us/DDanchev/MAC>
78. <http://www.mapsofwar.com/ind/american-wars.html>
79. <http://del.icio.us/DDanchev/Military>
80. <http://del.icio.us/DDanchev/War>
81. <http://del.icio.us/DDanchev/Leadership>

82.

[http://www.theregister.co.uk/2006/11/02/diebold\\_hacking\\_democracy/](http://www.theregister.co.uk/2006/11/02/diebold_hacking_democracy/)

83. <http://del.icio.us/DDanchev/Security>

84. <http://del.icio.us/DDanchev/Diebold>

85. <http://del.icio.us/DDanchev/Voting>

580



## The Blogosphere and Splogs (2006-11-07 23:38)

[1]

Just read Technorati's latest "[2]State of the Blogosphere, October, 2006"

presented with in-depth visual stats on the **57 million blogs** they're currently tracking, and yes, all the splogs they're fighting to filter. Worth taking your time to go through the post, and you may also be interested in finding how come

my [3]ROI out of blogging is so positive these days.

" As we've said in the past, some of the new blogs in our index are Spam blogs or '[4] splogs'. The good news is Technorati has gotten much better at preventing these kinds

*of blogs from getting into our indexes in the first place, which may be a factor in the slight slowing in the average of new blogs created each day.*

*The spikes in red on the chart above shows the increased activity that occurs when spammers create massive*

*numbers of fake blogs and try to get them into our indexes. As the chart shows, we've done a much better job over*

*the last quarter at nearly eliminating those red spikes.*

***While last quarter I reported about 8 % of new blogs that get***

***past our filters and make it into the index are splogs, I'm happy to report that that number is now more like 4 %.***

*As always, we'll continue to be hyper-focused on making sure that new attacks are spotted and eliminated as quickly as possible.*

*My gut feeling is that since we're better at dealing with Spam now, even some of the blue areas in last quar-*

*ter's graph were probably accountable to spam, which would mean that rather than the bumpy ride shown above,*

*we're actually seeing a steady increased (but slower) growth of the blogosphere. Hopefully we'll be able to have a more detailed analysis of these issues next quarter."*

Meanwhile, the [5]splogfigher is doing an amazing job of analyzing and coming up with exact splog URLs - I'm repost-



ing so that third-parties of particular interest reading here take a notice – and week ago came up with [6]150,000

splogs, notice the dominating blogging platform? Blogspot all the way!

*" I see that Google has been deleting quite a large number of splogs but even then they are on average about 20 %*

*effective. What that means is if a single spammer creates 1000 splogs, Google will eventually delete at most about*

*200 of them leaving 800 alone. Obviously this is rather poor percentage and hopefully my efforts will bump up that*

*figure close to 90 % and above. [7] 20061030\_1.txt- 19401 splogs*

[8] 20061030\_2.txt- 4332 splogs

[9] 20061030\_3.txt- 8936 splogs

[10] 20061030\_4.txt- 8794 splogs

[11] 20061030\_5.txt- 18912 splogs

[12] 20061030\_6.txt- 5158 splogs

[13] 20061030\_7.txt- 70755 splogs

[14] 20061030\_8.txt- 1182 splogs

[15] 20061030\_9.txt- 11410 splogs

[16] 20061030\_10.txt- 968 splogs

[17] 20061030\_11.txt- 1584 splogs

*Here is a tarball of all splog list files listed above: [18]  
20061030.tar.gz"*

581

Obviously, spammers are exploiting Blogspot's [19]signup process, and I really feel it's about time Google starts tolerating more errors with users having trouble reading a sophisticated CAPTCHA, compared to its current too

user-friendly and [20]easily defeated one. They can balance for sure. Something else to consider, take for example

the [21]splogs collected for May, and whole the splogfighter is pointing out on the engineered 404s and Google's

efforts in removing them, I was able to verify content response from over 200 splogs reported back then, take

**cigar-accessories-2008.blogspot.com** for instance – anyone up for crawling the lists and clustering the results? Once the signup process is flawed, not even the wisdom of crowds flagging splogs can help you.

Another recommended and very recent analysis "[22]Characterizing the Splogosphere" is also full of juicy details, and statistical info on the emerging problem. Spammers are anything but old-fashioned.

1.

<http://photos1.blogger.com/blogger2/4099/2257/1600/Slide0004-10.gif>

2. <http://technorati.com/weblog/2006/11/161.html>

3. <http://ddanchev.blogspot.com/2006/10/return-on-investment-of-blogging.html>
4. <http://en.wikipedia.org/wiki/Splog>
5. <http://fightsplog.blogspot.com/>
6. <http://fightsplog.blogspot.com/2006/10/big-batch-of-splogs.html>
7. [http://desplog.org/txt/2006/10/30/20061030\\_1.txt](http://desplog.org/txt/2006/10/30/20061030_1.txt)
8. [http://desplog.org/txt/2006/10/30/20061030\\_2.txt](http://desplog.org/txt/2006/10/30/20061030_2.txt)
9. [http://desplog.org/txt/2006/10/30/20061030\\_3.txt](http://desplog.org/txt/2006/10/30/20061030_3.txt)
10. [http://desplog.org/txt/2006/10/30/20061030\\_4.txt](http://desplog.org/txt/2006/10/30/20061030_4.txt)
11. [http://desplog.org/txt/2006/10/30/20061030\\_5.txt](http://desplog.org/txt/2006/10/30/20061030_5.txt)
12. [http://desplog.org/txt/2006/10/30/20061030\\_6.txt](http://desplog.org/txt/2006/10/30/20061030_6.txt)
13. [http://desplog.org/txt/2006/10/30/20061030\\_7.txt](http://desplog.org/txt/2006/10/30/20061030_7.txt)
14. [http://desplog.org/txt/2006/10/30/20061030\\_8.txt](http://desplog.org/txt/2006/10/30/20061030_8.txt)
15. [http://desplog.org/txt/2006/10/30/20061030\\_9.txt](http://desplog.org/txt/2006/10/30/20061030_9.txt)
16. [http://desplog.org/txt/2006/10/30/20061030\\_10.txt](http://desplog.org/txt/2006/10/30/20061030_10.txt)
17. [http://desplog.org/txt/2006/10/30/20061030\\_11.txt](http://desplog.org/txt/2006/10/30/20061030_11.txt)
18. <http://desplog.org/txt/2006/10/20061030.tar.gz>
19. <http://www.blogger.com/signup.g>
20. <http://sam.zoy.org/pwntcha/>

21. <http://fightsplog.blogspot.com/2006/05/big-batch-of-splogs.html>

22. <http://www.blogpulse.com/www2006-workshop/papers/splogosphere.pdf>

582



## **All Your Electromagnetic Transmissions Are Belong To Us (2006-11-09 17:07)**

[1]

This is [2]worth mentioning, as while you try not to talk about [3]these locations

for as long as someone doesn't start blowing the whistle too loud, all you really need is someone to pass by and feel

the hyper-sensitive harassment due to Trimingham's ELINT capabilities – and [4]news [5]articles [6]keep [7]coming

about this particular case.

*" The Ministry of Defence has admitted that a fault at a radar dome was responsible for causing electrical*

*problems with dozens of cars. Engines and lights cut out and speedometer dials swung up to 150mph as motorists*

*drove past the dome. At the time the MoD said there was no guarantee that the Trimingham radar on the north*

*Norfolk coast was the cause. "*

Read some of the memories of a serviceman that was stationed there [8]during the 60s :

*" Another story that might be of interest relates to the time that a Russian trawler went aground at Skaw. The*

*indications were that it was an Elint (Electronic intelligence gathering) vessel as the crew hid what they were doing from an RAF Shackleton which flew overhead as part of the search and rescue mission. Whether there was any*

*spying equipment on board is debatable. In any event, the Unst folk did well in "liberating" fishing nets and sundry bits and pieces including the steering wheel, which was subsequently returned to the Russians. However, two RAF*

*lads a steward and a cook found signals, maps and other papers in the skipper's cabin, some of this hidden under his mattress. They brought these back to me and our station intelligence officer had a look at them. By chance he was*

*a Russian linguist and was able to provide a summary of what was in the documents before they were forwarded to*

*the RAF intelligence staff at the Ministry of Defence. One of the documents proved extremely valuable to the Navy*

*but what amazed them was that the translated summary had been done by an RAF flying officer on Unst. "*

You may also be [9]interested in going through a table that *" includes all military sites which have significant intelligence-*

*gathering or analysis capability with official US presence; these are the sites which have figures for*

*numbers of US and UK personnel".*

Trimingham's radar dome courtesy of [10]munkto, and [11]Flickr's Radars group.

### **Related posts:**

[12]Why's that radar screen not blinking over there?

[13]Achieving Information Warfare Dominance Back in 1962

1.

[http://photos1.blogger.com/blogger2/4099/2257/1600/11067856\\_501ca5f04d.jpg](http://photos1.blogger.com/blogger2/4099/2257/1600/11067856_501ca5f04d.jpg)

2. <http://www.engadget.com/2006/11/08/uk-radar-station-causing-car-engine-and-electrical-troubles/>

3. [http://ddanchev.blogspot.com/2006/09/satellite-imagery-of-secret-or\\_28.html](http://ddanchev.blogspot.com/2006/09/satellite-imagery-of-secret-or_28.html)

4. <http://news.bbc.co.uk/1/hi/england/norfolk/6110844.stm>

5.

[http://www.guardian.co.uk/uk\\_news/story/0,,1714941,00.html](http://www.guardian.co.uk/uk_news/story/0,,1714941,00.html)

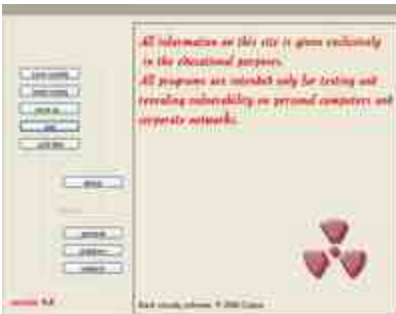
6.

[http://www.theregister.co.uk/2006/02/28/car\\_molesting\\_radar/](http://www.theregister.co.uk/2006/02/28/car_molesting_radar/)

7. <http://www.thisislondon.co.uk/news/article-23373150-details/Norfolk>

8. [http://www.shetlandtoday.co.uk/Shetlandtimes/content\\_details.asp?ContentID=18976](http://www.shetlandtoday.co.uk/Shetlandtimes/content_details.asp?ContentID=18976)
9. [http://www.staff.ncl.ac.uk/d.f.j.wood/thesis\\_app2.htm](http://www.staff.ncl.ac.uk/d.f.j.wood/thesis_app2.htm)
10. <http://flickr.com/photos/munkt0n/>
11. <http://www.flickr.com/groups/radars/>
12. <http://ddanchev.blogspot.com/2006/04/whys-that-radar-screen-not-blinking.html>
13. <http://ddanchev.blogspot.com/2006/08/achieving-information-warfare.html>

584



## The Nuclear Grabber Toolkit (2006-11-09 21:32)

[1]

In case you're unaware of [2]Nuclear Grabber's existence - [3]Babelfish it

-WebSense commented on it in their latest "[4]Security Trends - first half of 2006 report" :

*" Another toolkit example is Nuclear Grabber, which allows an attacker to sit on a real banking site and grab data from electronic forms. Like WebAttacker, this tool is available on Russian websites. The cost of Nuclear Grabber is a hefty \$3,000. "*

It's actually "3250 USD for a server size of 50-53kb" as the site says - perceived pricing and profit margins greed thankfully ruin its popularity from my point of view. Advanced [5]form grabbers like this one are always very ugly -

tavarish chto vui being so [6]knowledgeable, yet so malicious messing up with the entry barriers in this space?!

[7]

[8]Full scale automation in [9]action, quite some infected folks geolocated al-

ready. Going to wash my hands now..

1. <http://photos1.blogger.com/blogger2/4099/2257/1600/nuclear1.png>

2. <http://corpsespyware.net/nuclear.htm>

3. <http://babelfish.altavista.com/>



4. [http://www.websense.com/securitylabs/docs/WebsenseSecurityLabs20061H\\_Report.pdf](http://www.websense.com/securitylabs/docs/WebsenseSecurityLabs20061H_Report.pdf)
5. <http://corpsespyware.net/exmpl.htm>
6. <http://www.corpsespyware.net/tech.htm>
7. <http://photos1.blogger.com/blogger2/4099/2257/1600/adm2.png>
8. <http://mazafaka.biz/adm.rar>
9. [http://www.bleedingthreats.net/cgi-bin/viewcvs.cgi/sigs/MALWARE/MALWARE\\_Corpsespyware?rev=1.7](http://www.bleedingthreats.net/cgi-bin/viewcvs.cgi/sigs/MALWARE/MALWARE_Corpsespyware?rev=1.7)

585



## **Bill Gates on Traffic Acquisition and Internet Bubbles (2006-11-13 01:23)**

[1]

Confused [2]Bill Gates, but a regularly attacked one too. A rather predictable

comment given he's not the only one selling the chewing gums and the soaps this time, so keep on bubbling folks.

Think mature Web 2.0, think [3]Semantic web, or at least dare to envision – Microsoft wishes the Internet was never invented, unless of course they could sell you the license to use it.

*" There are a hundred YouTube sites out there," Gates said during an interview with a group of journalists in Brussels before a speech to European lawmakers. "You never know. It's very complicated in terms of what are the business models for these sites." Some of them, including sites that offer Web-based word processing and search engines, are being promoted by their creators and analysts as possible competitors to makers of retail packaged*

*software like Microsoft. "We're back kind of in Internet-bubble era in terms of people thinking: 'O.K., traffic. We want traffic. We want traffic,'" Gates said. "There are still some areas where it is unclear what's going to come out of that. "*

The very basics of Internet marketing which transform branding into communication, segments into communi-

ties for instance doesn't necessarily mean that traffic is the cornerstone of E-business. Eyeballs, thus participants

merely visitors converted into revenue sources speak for themselves. Win-win-win business models need no

comment. Once you get the traffic, boy, what wonders are there for you to discover, sense and profitably respond

to. But then again, keep in mind that search and online video represent a tiny portion of the overall Internet user's

activities. **Don't look for the next Google, or the next YouTube, look beyond.**

Having R &D centers on [4]enemy territories creates more job opportunities, and improves Microsoft's com-

fortability with its stakeholders :

*" Microsoft said that it would invest \$7.8 billion globally in research and development this year, about 15 percent of sales, and it plans to spend \$500 million in Europe next year. Microsoft operates its main European research center on the campus of Cambridge University in England, with other research offices in Denmark and Ireland. "*

While it's also cheaper to operate them in Europe than in the U.S, [5]money cannot buy innovation and [6]many

other things, so don't get [7]too excited but learn [8]how to surf tidal waves, the ones Bill Gates himself predicted

back in 1995.

### **Related posts:**

[9]5 things Microsoft can do to secure the Internet, and why it wouldn't?

[10]Microsoft in the Information Security Market

[11]Microsoft's OneCare Penetration Pricing Strategy

1.

[http://photos1.blogger.com/blogger2/4099/2257/1600/Microsoft\\_Live.jpg](http://photos1.blogger.com/blogger2/4099/2257/1600/Microsoft_Live.jpg)

2. <http://www.ecommercetimes.com/rsstory/54202.html>

3. [http://en.wikipedia.org/wiki/Semantic\\_Web](http://en.wikipedia.org/wiki/Semantic_Web)
4. <http://www.crn.com.au/story.aspx?CIID=68214&src=site-marq>
5. [http://photos1.blogger.com/blogger/1933/1779/1600/RD\\_spending.jpg](http://photos1.blogger.com/blogger/1933/1779/1600/RD_spending.jpg)
6. <http://ddanchev.blogspot.com/2006/07/things-money-cannot-buy.html>
7. [http://money.cnn.com/2006/03/30/news/newsmakers/gates\\_howework\\_fortune/](http://money.cnn.com/2006/03/30/news/newsmakers/gates_howework_fortune/)
8. <http://www.businessweek.com/1996/29/b34842.htm>
9. <http://ddanchev.blogspot.com/2006/03/5-things-microsoft-can-do-to-secure.html>
10. <http://ddanchev.blogspot.com/2006/05/microsoft-in-information-security.html>
11. <http://ddanchev.blogspot.com/2006/08/microsofts-onecare-penetration-pricing.html>

586

587

x

## **Jihadi PSYOPS - CIA Attacks on Terrorist Websites (2006-11-13 03:42)**

Last week, the Internet Haganah [1]reported on rumors around jihadist forums, namely, that the [2]CIA has been

attacking jihadi web sites.

Now while this is [3]totally untrue – the CIA would rather be monitoring instead of shutting them down, or

shut them down only after they've gathered enough info – it's a good example of twisting the facts to improve the

productivity and self-esteem of the jihadists supposed to strike back.

1. <http://internet-haganah.org/harchives/005770.html>

2. <http://internet-haganah.org/harchives/005770.html>

3. <http://www.haganah.org.il/harchives/005774.html>

588

x

## **U.S No-Fly-List Enforced at Deutsche Bank NYC (2006-11-14 02:51)**

[1]

Apparently, the [2]no-fly-list has been recently used as an [3]access control measure at the Deutsche Bank's

NYC's office according to the DealBreaker :

*" We hear Deutsche Bank's super-suped-up security extends beyond just the beefy armed guards patrolling the*

*street outside its headquarters at 60 Wall. Yesterday apparently a consultant who was scheduled to attend a meeting*

*at the bank was denied entry because his name appears on the federal "no fly" list. "It was the most intense security I've seen, except for maybe the Israeli consulate," a source who was present when the consultant was denied entry tells DealBreaker. "*

While that's a very unpragmatic paranoia, a [4]U.S congresswoman seems to have recently experienced the "no-fly-list trip" too :

*" Sanchez said her staff had booked her a one-way ticket from Boise, Idaho to Cincinnati through Denver. Her*

*staff, however, was prevented from printing her boarding pass online and were also blocked from printing her*

*boarding pass at an airport kiosk. Sanchez said she was instructed to check in with a United employee, who told her*

*she was on the terrorist watch list. The employee asked her for identification, Sanchez recalled. "I handed over my congressional ID and he started laughing and said, 'I'm going to need an ID that has your birthday on it,'" Sanchez said in a phone interview with The Associated Press. The employee used Sanchez's birth date to determine that she*

*was not the same Loretta Sanchez listed in the database and she was able to board her flight, she said. "*

[5]Bureaucrats don't just slow down innovation and take credit for it, but when they also fall down from a window it takes a week for them to hit the ground.

1. [http://photos1.blogger.com/blogger2/4099/2257/1600/common\\_sense.jpg](http://photos1.blogger.com/blogger2/4099/2257/1600/common_sense.jpg)
2. [http://en.wikipedia.org/wiki/No-fly\\_list](http://en.wikipedia.org/wiki/No-fly_list)
3. [http://www.dealbreaker.com/2006/11/no\\_fly\\_means\\_no\\_entry\\_at\\_deuts.php](http://www.dealbreaker.com/2006/11/no_fly_means_no_entry_at_deuts.php)
4. <http://www.sfgate.com/cgi-bin/article.cgi?file=/news/archive/2006/10/30/state/n174752S39.DTL>
5. <http://ddanchev.blogspot.com/2006/03/are-cyber-criminals-or-bureaucrats.html>

589

x

## Satellite Imagery Trade-offs (2006-11-14 03:37)

[1]

Informative to know :

" Eventually, Andersen said, the big but light telescopes could solve a spy-satellite conundrum. **Now, those camera**

**equipped satellites must fly closer to Earth to generate usable pictures. That means their orbits exceed the speed**

**of Earth's rotation, so the satellites cannot spend much time photographing one location.** If spy satellites had huge telescopes, they could be placed higher above the planet in an orbit that moves at the same speed as Earth's

*rotation, so they could photograph the same region constantly. "*

There's just one tiny comment that makes a bad impression -  
*"That way, you could keep a constant eye on someone*

*like Osama bin Laden"* he said." In exactly the say way a security consultant wrongly tries to talk top management into increasing a budget by using the buzzword cyberterrorism, it wouldn't work and it's a rather desperate move. Even

though, in case you're interested in keeping track of Bin Laden's desert trips, make sure you add a detection pattern

for a [2]white horse riding through Afghanistan. Go through some of my previous posts to catch up [3]with [4]my

[5]comments on [6]related [7]topics.

1. <http://www.gazette.com/display.php?id=1325576&secid=1>

2. <http://www.zmag.org/content/showarticle.cfm?ItemID=2622>

3. <http://ddanchev.blogspot.com/2006/09/benefits-of-open-source-intelligence.html>

4. <http://ddanchev.blogspot.com/2006/09/stealth-satellites-developments-source.html>

5. <http://ddanchev.blogspot.com/2006/10/history-and-future-of-us-military.html>

6. <http://ddanchev.blogspot.com/2006/07/japans-reliance-on-us-spy-satellites.html>



7. <http://ddanchev.blogspot.com/2006/07/open-source-north-korean-imint.html>

590

x

## **Widener University Forensics Course (2006-11-14 04:02)**

[1]

Just noticed that the [2]reading materials for the course are also listing my "[3]Steganography and Cyber

Terrorism Communications" post. [4]Looks nice!

1. <http://photos1.blogger.com/blogger2/4099/2257/1600/widener.jpg>

2. <http://cs.widener.edu/~yanako/html/courses/Fall06/forensics/coursemat.html>

3. <http://ddanchev.blogspot.com/2006/08/steganography-and-cyber-terrorism.html>

4. <http://ddanchev.blogspot.com/2006/07/security-research-reference-coverage.html>

591

x



## **London's Police Experimenting with Head-Mounted Surveillance Cameras (2006-11-20 20:35)**

[1]

[2]Innovative, but a full scale violation of [3]privacy – what privacy with walking CCTVs nowadays?!

*" The world draws ever-closer to the dystopia imagined in Hollywood blockbusters – police in London are to be*

*equipped with [4] head-mounted cameras which will record everything in the direction the officer is looking. The tiny cameras are about the size of an AA battery and can record images of an extremely high quality.*

*Claimed to be a deterrent for anti-social behaviour, the first run of head-cams are being tested by eight Metropolitan beat officers this month. If successful, all police officers will eventually be equipped with a head camera.*

*These new 'robocops' add to the growing number of surveillance machines that peer at the public. **Cynics ar-***

***gue that the logical progression of the police head-cam will be head-cameras that all citizens are required to wear.***

*The video data would be relayed back to a central database where transgressions are recorded by a computer. "*

[5]George Orwell is definitely turning upside down in his grave in the time of writing, and it's entirely up to

you to come up with the possible scenarios for abusing this innovation – [6]The Final Cut too, has a good perspective.

Think that's not enough to raise your eyebrows? [7]British Telecom is also about to " **put thousands of spy**

***camera recorders in its phone boxes and beam suspects mugshots to police. Cameras stationed on top of lamp-***

***posts near the kiosks will send images to hidden digital video recorders inside the booths. Suspects photos will then be messaged almost instantly to hand-held digital assistants used by police and emergency services. "***

### **Issues to keep in mind:**

- No more tax payers' money wasted on CCTVs to only cover the blind spots introduced by the old ones, now you

have the "walking CCTVs" taking care

- Face and voice recognition, as well as parabolic type of remote listening capabilities will be the next milestones to reach

- Data collected would prove invaluable to ongoing investigations, and you know, "computers never lie" so digitally introducing minor motives here and there becomes a handy weakness

- More entertaining reality shows will follow for the purpose of communicating the value of the cameras to the general public

- Someone will sooner or later find a way to jam the stream

[8]

There's a saying about not looking anyone straight into the eyes on the

mean streets of New York, guess the same applies to not looking straight into the eyes of London's police anymore.

[9]Every country needs an [10]EFF of its own, [11]especially the U.K these days. To illustrate what I have in mind,

[12]EPIC's listing the U.K at the top of the leading EU surveillance societies, and you may also find the [13]U.K's

opinion on its state of total surveillance, informative as well.

Finger-mounted keyboard chick courtesy of [14]Kittytech.

1.

<http://crave.cnet.co.uk/camcorders/0,39029423,49285395,00.htm>

592

2.

<http://crave.cnet.co.uk/camcorders/0,39029423,49285395,00.htm>

3. <http://del.icio.us/DDanchev/Privacy>

4. <http://www.egovmonitor.com/node/8662>

5. [http://en.wikipedia.org/wiki/Nineteen\\_Eighty-Four](http://en.wikipedia.org/wiki/Nineteen_Eighty-Four)

6. <http://ddanchev.blogspot.com/2006/08/dvd-of-weekend-final-cut.html>

7. [http://www.mirror.co.uk/news/tm\\_headline=eye-spy-in-every-bt-phone-box-&method=full&objectid=18123366&siteid=94762-name\\_page.html](http://www.mirror.co.uk/news/tm_headline=eye-spy-in-every-bt-phone-box-&method=full&objectid=18123366&siteid=94762-name_page.html)

8.

<http://photos1.blogger.com/x/blogger2/4099/2257/1600/57984/phr2005spread.jpg>

9. <http://www.edri.org/>

10. <http://www.eff.org/>

11. <http://spyblog.org.uk/>

12. <http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-545223>

13.

[http://www.ico.gov.uk/upload/documents/library/data\\_protection/practical\\_application/surveillance\\_society](http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society)

[\\_full\\_report\\_2006.pdf](#)

14. <http://www.kittytech.com/>

593



## **How to Tell if Someone's Lying to You (2006-11-27 04:31)**

[1]

Interactive slideshow providing ten tips on how to tell if someone's lying to you.

These can of course be interpreted in different ways and applied under specific circumstances only. Some are very

practical though :

01. **Watch Body Language**
02. **Seek Detail**
03. **Beware Unpleasantness**
04. **Observe Eye Contact**
05. **Signs of Stress**
06. **Listen for the Pause**
07. **Ask Again**
08. **Beware Those Who Protest Too Much**
09. **Know Thyself**
10. **Work on Your Intuition**

Two more I can add – **answering without being asked**, and **on purposely stating the possibility as a negative**

**statement already**. Here's [2]the article itself, as well as several more [3]handy tips on [4]detecting lies. Don't forget

- if someone's being too nice with you, it means they're beating you already.

Ear whisper courtesy of [5]Cartoonstock.com

1. [http://www.forbes.com/2006/11/02/tech-cx\\_ee\\_technology\\_liar\\_slide.html?boxes=custom](http://www.forbes.com/2006/11/02/tech-cx_ee_technology_liar_slide.html?boxes=custom)

2. [http://www.forbes.com/technology/2006/11/03/detecting-lies-trust-tech\\_06trust\\_cx\\_ee\\_1103lies.html](http://www.forbes.com/technology/2006/11/03/detecting-lies-trust-tech_06trust_cx_ee_1103lies.html)

3. <http://www.apa.org/monitor/julaug04/detecting.html>

4. <http://www.bbc.co.uk/dna/h2g2/A664021>

5. <http://www.cartoonstock.com/>

594



## **To Publish a Privacy Policy or Not to Publish a Privacy Policy (2006-11-27 04:45)**

[1]

Here's an article arguing that "[2]publishing a privacy statement may be more

harmful than not publishing one"only if enforcement, implementation and monitoring don't intersect as they should :

*" This case demonstrates a complication relating to companies' claiming that they have security measures to protect their end users' privacy. Large, established companies, like Eli Lilly, understand this issue but may still have problems ensuring compliance to their privacy policy. **But many emerging companies immediately post their***

***claimed privacy policies on their company websites. These companies often fail to assess the potential risks,***

***burdens and liabilities associated with publishing a privacy policy. They do not realize that publishing a privacy***

***statement may be more harmful than not publishing one. "***

Privacy exposure assessments still remain rather unpopular among leading companies, and compliance with

industry specific requirements for processing and storing personal information continue indirectly replacing what

a Chief Privacy Officer would have done in a much more adaptive manner. Can we that easily talk about **Total**

**Privacy Management (TPM)**, the way talk about **Total Quality Management (TQM)** as an internal key objective

for strengthening a company's reputation as a socially-oriented one? It would definitely turn into a criteria for the

stakeholders, and a differentiating point for any company in question in the long term. [3]The future of privacy?

[4]Don't over-empower the watchers or you'll have the entire data aggregation model of our society used [5]against

your rights for the sake of protecting you from " **the enemy or the threat of the day**".

You may also find some comments from a previous post on " [6]Examining Internet Privacy Policies" relevant

to the topic :

*" Accountability, public commitment, or copywriters charging per word, privacy policies are often taken for fully enforced ones, whereas the truth is that actually no one is reading, bothering to assess them. And why would you, as by the time you've finished you'll again have no other*



*choice but to accept them in order to use the service in question*

*- too much personal and sensitive identifying information is what I hear ticking. That's of course the privacy conscious perspective, and to me security is a matter of viewpoint, the way you perceive it going beyond the basics, the very*

*same way you're going to implement it - Identity 2.0 as a single sign on Web is slowly emerging as the real beast."*

1.

<http://photos1.blogger.com/blogger2/4099/2257/1600/brainwashing.jpg>

2. <http://www.csoonline.com/caveat/092506.html>

3. <http://ddanchev.blogspot.com/2006/03/future-of-privacy-dont-over-empower.html>

4. <http://ddanchev.blogspot.com/2006/03/data-mining-terrorism-and-security.html>

5. <http://ddanchev.blogspot.com/2006/03/security-vs-privacy-or-whats-left-from.html>

6. <http://ddanchev.blogspot.com/2006/09/examining-internet-privacy-policies.html>

595



**Global Map of Security Incidents and Terrorist Events  
(2006-11-27 05:39)**

[1]

Outstanding project demonstrating [2]the benefits of open source intelligence positioned on Google Maps

while providing you with the very latest global security and suspicious events in categories such as :

- **Airport/Aviation Incidents**
- **Arson/Fire Incidents**
- **Biological Incidents/ Threats/ Anthrax Hoaxes etc**
- **Bomb Incidents/Explosives/ Hoax Devices**
- **Chemical Incident**
- **Dam Incident**
- **Radiation Incidents/ Smuggling/ Proliferation**
- **Chemical Attack**
- **Other Suspicious Activity**
- **Shipping/Maritime/Ports/Cargo/Waterways Security**
- **Assassination/ Assassination Attempt**
- **Railways/Train Stations**
- **Bus Stations/ Bus Security/ Bus Related Incidents**
- **Bridge / Tunnel Incidents and Security**
- **Shootings / Sniper Incidents/ Etc**
- **Terrorist Arrests/Captured/Killed Locations**

No more "slicing the threat on pieces", now you can see the big picture for yourself.

1. <http://www.globalincidentmap.com/home.php>
2. <http://ddanchev.blogspot.com/2006/09/benefits-of-open-source-intelligence.html>

596

x

## **How to Fake Fingerprints (2006-11-27 06:24)**

[1]

With all the buzz of [2]fingerprinting this and [3]that, fingerprint these [4]instructions on how copy and fake

fingerprints :

*" In order to fake a fingerprint, one needs an original first. Latent fingerprints are nothing but fat and sweat on touched items. Thus to retrieve someone elses fingerprint (in this case the fingerprint you want to forge) one*

*should rely on well tested forensic research methods. Which is what's to be explained here. "*

Bow to the CCC's full disclosure shedding more light on a common sense insecurity. While it can be tackled

by both ensuring the quality of the fingerprinting process, and by technological means such as adding extra layers or

cross-referencing through different databases, multiple-factor authentication's benefits are proportional with their

immaturity and usability issues. Fancy? For sure. Cutting-edge security? Absolutely from a technological point of

view. But when fingerprints start getting more empowerment and integration within our daily lives, malicious parties

would have already taken notice, and again be a step ahead of the technological bias on fingerprinting. Coming up

with new identities may indeed end up as a commodity neatly stored in a central database, or perhaps ones collected

from elsewhere.

1.

[http://photos1.blogger.com/x/blogger2/4099/2257/1600/697161/small\\_06-finger+nachbearbeiten.png](http://photos1.blogger.com/x/blogger2/4099/2257/1600/697161/small_06-finger+nachbearbeiten.png)

2. <http://ddanchev.blogspot.com/2006/10/surveillane-system-about-to-get.html>

3. <http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2006/11/22/ufingers122.xml>

4. [http://www.ccc.de/biometrie/fingerabdruck\\_kopieren.xml?language=en](http://www.ccc.de/biometrie/fingerabdruck_kopieren.xml?language=en)

597



**Video of Birds Attacking an Unmanned Aerial Vehicle (UAV) (2006-11-29 17:13)**

[1]

Mother Nature on the basics of asymmetric warfare :

*" However, on one flight, a test Raven attracted the attention of two nearby crows, who initially squawked a territorial warning at the UAV. Unsuprisingly undeterred by the warnings, the UAVs carried on on their descent and were subsequently attacked by the crows. See the video clip below.*

*The UAVs were required to remain at low altitude for the duration of each sortie, airspace above the city forming part of the western approaches to Brisbane International airport.*  
"

And no, don't even think on [2]speculating of [3]terrorists training divisions of crows to attack, or early warn of UAVs flying around the birds' air space, unless of course your wild imagination prevails.

1.

<http://www.flightglobal.com/Articles/2006/11/21/Navigation/177/210744/Video+When+the+birds+strike+-+crows+attack+Aerovironment+Raven+UAV+on+test+flight+over.htm>

2. [http://ddanchev.blogspot.com/2006/09/leaked-unmanned-aerial-vehicle-photo\\_18.html](http://ddanchev.blogspot.com/2006/09/leaked-unmanned-aerial-vehicle-photo_18.html)

3. <http://ddanchev.blogspot.com/2006/09/hezbollahs-use-of-unmanned-aerial.html>

598



## CIA Personality Quiz (2006-11-29 17:28)

[1]

An impressive mastermind is what I got as a type of personality, quite a bit of suspicious flattery isn't it?

I feel [2]the quiz is more of an ice-breaker, and it's hell of an amusing one as a matter of fact. Hint to the

CIA's HR department - promise to show the ones who make it up for a final interview a randomly chosen [3]analyst's

collection of secret UFO files, and see your conversion rates skyrocketing. Then explain them the basics of access

programs based on classification and why they have to perform better. Arbeit macht access to secret UFO files as a

factor for productivity, cute.

More comments from another wannabe [4]secret AGent.

1.

<http://photos1.blogger.com/x/blogger2/4099/2257/1600/292425/mastermind.jpg>

2. <https://www.cia.gov/careers/CIAMyths.html>

3. <http://ddanchev.blogspot.com/2006/08/analyzing-intelligence-analysts.html>

4.

[http://blogs.usatoday.com/techspace/2006/11/secret\\_agent.html](http://blogs.usatoday.com/techspace/2006/11/secret_agent.html)



## **A Movie About Trusted Computing (2006-11-30 18:10)**

[1]

Great [2]opinionated introduction to the [3]topic. Trusted computing isn't the

panacea of total security simply because [4]there can never be 100 % secure OS or a device, unless of course you put

so much security layers in place to end up with zero usability, so what's it gonna be? Insecurities are a commodity,

but security and usability issues are always a matter of viewpoint, so don't act as if you can provide 100 % security,

because what you're actually offering is a marginal thinking while proposing a solution.

1. [http://photos1.blogger.com/x/blogger2/4099/2257/1600/395049/trusted\\_computing.jpg](http://photos1.blogger.com/x/blogger2/4099/2257/1600/395049/trusted_computing.jpg)

2. <http://www.lafkon.net/tc/>

3. [http://en.wikipedia.org/wiki/Trusted\\_computing](http://en.wikipedia.org/wiki/Trusted_computing)

4. <http://www.securityabsurdity.com/failure.php>

600



## **A Chart of Personal Data Security Breaches 2005-2006 (2006-11-30 18:31)**

[1]

Following my previous post on "[2]Personal Data Security Breaches - 2000/2005",

you may also find this "[3]Chart of Security Breaches for 2005 - 2006" worth taking a look at – lost or stolen equipment with data dominate the threatscape.

With the eye-popping big bubbles, and hundreds of thousands of people exposed due to the centralized and insecure

nature of storing and processing their information, ask yourself why would an attacker ever bother to initiate a network level attack against a data aggregator nowadays? Consider the other perspective when it comes to data security

breaches, namely "[4]To report, or not to report?" a breach, and how is an organization supposed to report when they're not even aware that personal information has already been exposed.

Take your time to go through a very good resource keeping track of [5]all reported data security breaches and notice

the most common patterns for yourself.

1.

[http://photos1.blogger.com/x/blogger2/4099/2257/1600/431813/chart\\_breaches.jpg](http://photos1.blogger.com/x/blogger2/4099/2257/1600/431813/chart_breaches.jpg)

2. <http://ddanchev.blogspot.com/2006/01/personal-data-security-breaches.html>



3. <http://www.consumerist.com/consumer/identity-theft/pictorial-guide-to-this-year-in-personal-id-breaches-214860.php>

4. <http://ddanchev.blogspot.com/2006/01/to-report-or-not-to-report.html>

5. <http://www.numbrx.net/>

601

**2.12**

**December**

602



### **Symantec's Invisible Burglar Game (2006-12-07 15:45)**

Cheers to Symantec's PR folks for coming up with such an [1]entertaining promotion of Norton 360, so that " *if*

*everything gets too much hit the spacebar to activate the Norton 360 force field to destroy everything in sight. "*

Good one!

Try the infamous [2]Airport security flash game too, and search everyone for exploding toothpastes, and other

dangerous substances as they become dangerous throughout the game.

1. <http://www.symantec.com/invisibleburglar>

2. <http://ddanchev.blogspot.com/2006/09/airport-security-flash-game.html>

603



## **Symantec's Invisible Burglar Game (2006-12-07 16:46)**

[1]

Cheers to Symantec's PR folks for coming up with such an [2]entertaining promotion of Norton 360, so that " *if*

*everything gets too much hit the spacebar to activate the Norton 360 force field to destroy everything in sight. "*

Good one!

Try the infamous [3]Airport security flash game too, and search everyone for exploding toothpastes, and other

dangerous substances as they become dangerous throughout the game.

1.  
[https://web.archive.org/web/20101016192214/http://4.bp.blogspot.com/\\_wICHhTiQmrA/RXgbS9wujAI/AAAAAAAAAE4/1g6\\_uOK1FAo/s1600-h/mission1.jpg](https://web.archive.org/web/20101016192214/http://4.bp.blogspot.com/_wICHhTiQmrA/RXgbS9wujAI/AAAAAAAAAE4/1g6_uOK1FAo/s1600-h/mission1.jpg)

2. <http://www.symantec.com/invisibleburglar>

3. <http://ddanchev.blogspot.com/2006/09/airport-security-flash-game.html>

604

# Document Outline

- 2005
  - December
    - [How to create better passwords - why bother?! \(2005-12-07 16:43\)](#)
    - [Obay - how realistic is the market for security vulnerabilities? \(2005-12-12 16:40\)](#)
    - [IP cloaking and competitive intelligence/disinformation \(2005-12-14 16:36\)](#)
    - [Insiders - insights, trends and possible solutions \(2005-12-19 12:22\)](#)
    - [Cyberterrorism - don't stereotype and it's there! \(2005-12-19 15:27\)](#)
    - [Insiders - insights, trends and possible solutions \(2005-12-19 15:33\)](#)
- [2006](#)
  - [January](#)
    - [What's the potential of the IM security market? Symantec thinks big \(2006-01-04 12:18\)](#)
    - [Keep your friends close, your intelligence buddies closer! \(2006-01-04 13:11\)](#)
    - [Security quotes : a FSB \(successor to the KGB\) analyst on Google Earth \(2006-01-04 13:38\)](#)
    - [How to secure the Internet \(2006-01-04 14:22\)](#)
    - [Happy New Year folks!! \(2006-01-04 17:15\)](#)
    - [What's the potential of the IM security market? Symantec thinks big \(2006-01-04 17:17\)](#)
    - [Keep your friends close, your intelligence buddies closer! \(2006-01-04 17:18\)](#)
    - [Security quotes : a FSB \(successor to the KGB\) analyst on Google Earth \(2006-01-04 17:19\)](#)
    - [How to secure the Internet \(2006-01-04 17:21\)](#)

- [Malware - future trends \(2006-01-09 17:22\)](#)
- [Watch out your wallets! \(2006-01-10 17:24\)](#)
- [Would we ever witness the end of plain text communications? \(2006-01-10 17:25\)](#)
- [Why we cannot measure the real cost of cybercrime? \(2006-01-10 17:28\)](#)
- [The never-ending "cookie debate" \(2006-01-10 17:30\)](#)
- [The hidden internet economy \(2006-01-11 17:39\)](#)
- [Security threats to consider when doing E-Banking \(2006-01-12 17:40\)](#)
- [Insecure Irony \(2006-01-12 17:42\)](#)
- [Future Trends of Malware \(2006-01-16 17:43\)](#)
- [To report, or not to report? \(2006-01-16 17:45\)](#)
- [Anonymity or Privacy on the Internet? \(2006-01-16 17:47\)](#)
- [What are botnet herds up to? \(2006-01-17 17:48\)](#)
- [China - the biggest black spot on the Internet's map \(2006-01-17 17:49\)](#)
- [FBI's 2005 Computer Crime Survey - what's to consider? \(2006-01-19 17:51\)](#)
- [Why relying on virus signatures simply doesn't work anymore? \(2006-01-19 17:52\)](#)
- [2006 = 1984? \(2006-01-23 17:54\)](#)
- [Cyberterrorism - recent developments \(2006-01-23 17:57\)](#)
- [Still worry about your search history and BigBrother? \(2006-01-23 17:59\)](#)
- [Homebrew Hacking, bring your Nintendo DS! \(2006-01-23 18:00\)](#)
- [Visualization, Intelligence and the Starlight project \(2006-01-23 18:01\)](#)
- [The Feds, Google, MSN's reaction, and how you got "bigbrothered"? \(2006-01-24 18:03\)](#)

- [Security Interviews 2004/2005 - Part 1 \(2006-01-26 07:22\)](#)
- [Personal Data Security Breaches - 2000/2005 \(2006-01-26 18:04\)](#)
- [Skype to control botnets?! \(2006-01-26 18:13\)](#)
- [Security Interviews 2004/2005 - Part 3 \(2006-01-26 18:46\)](#)
- [Security Interviews 2004/2005 - Part 2 \(2006-01-26 19:31\)](#)
- [Twisted Reality \(2006-01-30 18:15\)](#)
- [How we all get Own3d by Nature at the bottom line? \(2006-01-30 18:17\)](#)
- [Was the WMF vulnerability purchased for \\$4000?! \(2006-01-30 18:18\)](#)
- [January's Security Streams \(2006-01-31 18:19\)](#)
- [February](#)
  - [Suri Pluma - a satellite image processing tool and visualizer \(2006-02-02 15:28\)](#)
  - [CME - 24 aka Nyxem, and who's infected? \(2006-02-02 15:32\)](#)
  - [What search engines know, or may find out about us? \(2006-02-03 15:33\)](#)
  - [The current state of IP spoofing \(2006-02-06 10:01\)](#)
  - [Hacktivism tensions \(2006-02-07 10:08\)](#)
  - [Security Awareness Posters \(2006-02-07 13:35\)](#)
  - [A top level espionage case in Greece \(2006-02-08 15:14\)](#)
  - [The War against botnets and DDoS attacks \(2006-02-09 15:44\)](#)
  - [Who needs nuclear weapons anymore? \(2006-02-09 16:29\)](#)
  - [Recent Malware developments \(2006-02-13 16:43\)](#)
  - [Look who's gonna cash for evaluating the maliciousness of the Web? \(2006-02-14 17:12\)](#)

- [Detecting intruders and where to look for \(2006-02-15 08:48\)](#)
- [A timeframe on the purchased/sold WMF vulnerability \(2006-02-15 19:03\)](#)
- [The end of passwords - for sure, but when? \(2006-02-16 19:15\)](#)
- [How to win 10,000 bucks until the end of March? \(2006-02-17 13:45\)](#)
- [Smoking emails \(2006-02-17 23:41\)](#)
- [DVD of the weekend - The Lone Gunmen \(2006-02-17 23:47\)](#)
- [Chinese Internet Censorship efforts and the outbreak \(2006-02-24 13:14\)](#)
- [Master of the Infected Puppets \(2006-02-24 14:37\)](#)
- [Give it back! \(2006-02-24 15:36\)](#)
- [One bite only, at least so far! \(2006-02-24 16:21\)](#)
- [DVD of the Weekend - The Outer Limits - Sex And Science Fiction Collection \(2006-02-25 20:35\)](#)
- [Get the chance to crack unbroken Nazi Enigma ciphers \(2006-02-27 10:49\)](#)
- [March](#)
  - [DVD of the \(past\) weekend \(2006-03-06 14:12\)](#)
  - [February's Security Streams \(2006-03-06 14:44\)](#)
  - [Anti Phishing toolbars - can you trust them? \(2006-03-06 16:04\)](#)
  - [Data mining, terrorism and security \(2006-03-06 19:53\)](#)
  - [5 things Microsoft can do to secure the Internet, and why it wouldn't? \(2006-03-06 20:21\)](#)
  - [The Future of Privacy = don't over-empower the watchers! \(2006-03-07 16:45\)](#)
  - [Where's my 0day, please? \(2006-03-07 21:22\)](#)

- [DVD of the Weekend - The Immortals \(2006-03-10 14:23\)](#)
- [Security vs Privacy or what's left from it \(2006-03-15 12:41\)](#)
- [Old physical security threats still working \(2006-03-16 17:50\)](#)
- [Getting paid for getting hacked \(2006-03-17 13:19\)](#)
- ["Successful" communication \(2006-03-17 14:39\)](#)
- [Is a Space Warfare arms race really coming? \(2006-03-20 21:47\)](#)
- [The Practical Complexities of Adware Advertising \(2006-03-21 13:10\)](#)
- [Privacy issues related to mobile and wireless Internet access \(2006-03-21 17:24\)](#)
- [DVD of the Weekend - War Games \(2006-03-27 14:44\)](#)
- [Are cyber criminals or bureaucrats the industry's top performer? \(2006-03-27 16:25\)](#)
- [Visualization in the Security and New Media world \(2006-03-31 11:36\)](#)
- [March's Security Streams \(2006-03-31 15:13\)](#)
- [April](#)
  - [Wanna get yourself a portable Enigma encryption machine? \(2006-04-03 13:12\)](#)
  - [The "threat" by Google Earth has just vanished in the air \(2006-04-05 17:39\)](#)
  - [Insider fined \\$870 \(2006-04-05 18:22\)](#)
  - [Securing political investments through censorship \(2006-04-05 18:59\)](#)
  - [Heading in the opposite direction \(2006-04-05 19:51\)](#)
  - ["IM me" a strike order \(2006-04-12 12:35\)](#)
  - [Catching up on how to lawfully intercept in the digital era \(2006-04-12 19:17\)](#)

- [On the Insecurities of the Internet \(2006-04-13 12:04\)](#)
- [Distributed cracking of a utopian mystery code \(2006-04-13 15:09\)](#)
- [Fighting Internet's email junk through licensing \(2006-04-14 19:18\)](#)
- [Would somebody please buy this Titan 1 ICBM Missile Base? \(2006-04-18 13:44\)](#)
- [Spotting valuable investments in the information security market \(2006-04-18 19:15\)](#)
- [Digital forensics - efficient data acquisition devices \(2006-04-20 17:23\)](#)
- [The anti virus industry's panacea - a virus recovery button \(2006-04-20 20:07\)](#)
- [Why's that radar screen not blinking over there? \(2006-04-24 15:39\)](#)
- [25 ways to distinguish yourself - and be happy? \(2006-04-24 17:45\)](#)
- [Wild Wild Underground \(2006-04-25 13:05\)](#)
- [In between the lines of personal and sensitive information \(2006-04-26 09:52\)](#)
- [DIY Marketing Culture \(2006-04-27 13:16\)](#)
- [A comparison of US and European Privacy Practices \(2006-04-27 14:27\)](#)
- [May](#)
  - [April's Security Streams \(2006-05-02 11:39\)](#)
  - [Biased Privacy Violation \(2006-05-03 13:37\)](#)
  - [Travel Without Moving - Typhoon Class Submarines \(2006-05-04 13:50\)](#)
  - [The Current State of Web Application Worms \(2006-05-04 14:50\)](#)
  - [Shaping the Market for Security Vulnerabilities Through Exploit Derivatives \(2006-05-08 20:47\)](#)
  - [The Cell-phone Industry and Privacy Advocates VS Cell Phone Tracking \(2006-05-09 15:19\)](#)



- [Wiretapping VoIP Order Questioned \(2006-05-09 20:17\)](#)
- [Snooping on Historical Click Streams \(2006-05-11 12:16\)](#)
- [Pass the Scissors \(2006-05-11 12:46\)](#)
- [Is Bin Laden Lacking a Point? \(2006-05-11 13:27\)](#)
- [Pocket Anonymity \(2006-05-11 14:07\)](#)
- [Travel Without Moving - Scratching the Floor \(2006-05-11 14:55\)](#)
- [Terrorist Social Network Analysis \(2006-05-12 20:09\)](#)
- [Valuing Security and Prioritizing Your Expenditures \(2006-05-15 14:16\)](#)
- [EMP Attacks - Electronic Domination in Reverse \(2006-05-16 14:21\)](#)
- [Insider Competition in the Defense Industry \(2006-05-16 14:49\)](#)
- [Techno Imperialism and the Effect of Cyberterrorism \(2006-05-16 15:20\)](#)
- [Travel Without Moving - Cheyenne Mountain Operations Center \(2006-05-22 17:16\)](#)
- [Nation Wide Google Hacking Initiative \(2006-05-23 18:21\)](#)
- [Espionage Ghosts Busters \(2006-05-23 18:35\)](#)
- [Arabic Extremist Group Forum Messages' Characteristics \(2006-05-23 18:56\)](#)
- [The Current, Emerging, and Future State of Hacktivism \(2006-05-23 19:06\)](#)
- [Bedtime Reading - The Baby Business \(2006-05-23 19:15\)](#)
- [Travel Without Moving - Korean Demilitarized Zone \(2006-05-27 19:51\)](#)
- [Aha, a Backdoor! \(2006-05-27 20:19\)](#)
- [Forgotten Security \(2006-05-27 20:35\)](#)

- [Delaying Yesterday's "0day" Security Vulnerability \(2006-05-27 20:47\)](#)
- [Who's Who in Cyber Warfare? \(2006-05-28 15:34\)](#)
- [No Anti Virus Software, No E-banking For You \(2006-05-30 17:33\)](#)
- [Microsoft in the Information Security Market \(2006-05-30 17:51\)](#)
- [Covert Competitive Intelligence \(2006-05-30 18:03\)](#)
- [The Global Security Challenge - Bring Your Know-How \(2006-05-30 18:16\)](#)
- [Healthy Paranoia \(2006-05-31 15:40\)](#)
- [June](#)
  - [May's Security Streams \(2006-06-03 12:29\)](#)
  - [Travel Without Moving - KGB Lubyanka Headquarters \(2006-06-04 17:26\)](#)
  - [Skype as the Attack Vector \(2006-06-04 17:52\)](#)
  - [Where's my Fingerprint, Dude? \(2006-06-06 19:25\)](#)
  - [Phantom Planes in the Skies \(2006-06-06 19:37\)](#)
  - [Bedtime Reading - Rome Inc. \(2006-06-08 17:21\)](#)
  - [An Over-performing Spammer \(2006-06-08 17:32\)](#)
  - [Brace Yourself - AOL to Enter Security Business \(2006-06-09 15:49\)](#)
  - [Unknowingly Becoming a Child Porn King \(2006-06-10 16:26\)](#)
  - [All Your Confidentiality Are Belong To Us \(2006-06-10 16:49\)](#)
  - [There You Go With Your Financial Performance Transparency \(2006-06-10 16:57\)](#)
  - [Going Deeper Underground \(2006-06-10 17:11\)](#)
  - [Travel Without Moving - Georgi Markov's KGB Assassination Spot \(2006-06-11 16:15\)](#)

- [It's Getting Cloudy, and Delicious \(2006-06-11 16:31\)](#)
- [Consolidation, or Startups Popping out Like Mushrooms? \(2006-06-13 16:13\)](#)
- [Web Application Email Harvesting Worm \(2006-06-13 17:40\)](#)
- [No Other Place Like 127.0.0.1 \(2006-06-24 04:36\)](#)
- [Travel Without Moving - Erasmus Bridge \(2006-06-25 18:33\)](#)
- [Delicious Information Warfare - 13/24 June \(2006-06-25 19:41\)](#)
- [World's Internet Censorship Map \(2006-06-26 00:16\)](#)
- [Big Brother in the Restroom \(2006-06-26 01:09\)](#)
- [Dealing with Spam - The O'Reilly.com Way \(2006-06-26 15:23\)](#)
- [Shots From the Wild - Terrorism Information Awareness Program Demo Portal \(2006-06-27 03:54\)](#)
- [Malicious Web Crawling \(2006-06-27 17:34\)](#)
- [Delicious Information Warfare - 24/27 June \(2006-06-28 02:35\)](#)
- [Tracking Down Internet Terrorist Propaganda \(2006-06-29 03:27\)](#)
- [North Korea - Turn On the Lights, Please \(2006-06-29 03:56\)](#)
- [The WarDriving Police and Pringles Hacking \(2006-06-30 03:52\)](#)
- [Real-Time PC Zombie Statistics \(2006-06-30 04:56\)](#)
- [July](#)
  - [Hacktivism Tensions - Israel vs Palestine Cyberwars \(2006-07-01 17:18\)](#)
  - [China's Interest of Censoring Mobile Communications \(2006-07-02 02:53\)](#)

- [BBC under the Intelligence Shadow \(2006-07-03 00:57\)](#)
- [How to Win the U.S Elections \(2006-07-05 14:51\)](#)
- [Travel Without Moving - North Korea Missile Launch Pad \(2006-07-06 03:03\)](#)
- [\\$960M and the FBI's Art of Branding Insecurity \(2006-07-06 10:31\)](#)
- [Delicious Information Warfare - 27/07 \(2006-07-08 01:25\)](#)
- [Security Research Reference Coverage \(2006-07-09 18:27\)](#)
- [South Korea's View on China's Media Control and Censorship \(2006-07-10 22:21\)](#)
- [India's Espionage Leaks \(2006-07-10 23:36\)](#)
- [Spreading Psychological Imagination Streams \(2006-07-14 16:54\)](#)
- [North Korea's Cyber Warfare Unit 121 \(2006-07-16 01:08\)](#)
- [Scientifically Predicting Software Vulnerabilities \(2006-07-16 02:09\)](#)
- [Weaponizing Space and the Emerging Space Warfare Arms Race \(2006-07-16 14:50\)](#)
- [Malware Search Engine \(2006-07-17 23:06\)](#)
- [Open Source North Korean IMINT Reloaded \(2006-07-20 23:42\)](#)
- [Budget Allocation Myopia and Prioritizing Your Expenditures \(2006-07-21 00:43\)](#)
- [When Financial and Information Security Risks are Supposed to Intersect \(2006-07-21 01:30\)](#)
- [Anti Virus Signatures Update - It Could Wait \(2006-07-21 02:07\)](#)
- [Detailed Penetration Testing Framework \(2006-07-21 02:44\)](#)
- [Searching for Source Code Security Vulnerabilities \(2006-07-21 16:36\)](#)

- [An Intergalactic Security Statement \(2006-07-24 22:44\)](#)
- [Latest Report on Click Fraud \(2006-07-25 00:09\)](#)
- [Splitting a Botnet's Bandwidth Capacity \(2006-07-26 20:29\)](#)
- [The Beauty of the Surrealistic Spam Art \(2006-07-27 02:03\)](#)
- [DVD of the Weekend - Path to War \(2006-07-30 23:00\)](#)
- [Japan's Reliance on U.S Spy Satellites and Early Warning Missile Systems \(2006-07-31 02:14\)](#)
- [Things Money Cannot Buy \(2006-07-31 21:42\)](#)
- [August](#)
  - [But Of Course It's a Pleasant Transaction \(2006-08-02 15:02\)](#)
  - [One Time Password Generating Credit Card \(2006-08-03 01:39\)](#)
  - [Achieving Information Warfare Dominance Back in 1962 \(2006-08-03 19:36\)](#)
  - [Mobile Devices Hacking Through a Suitcase \(2006-08-04 04:27\)](#)
  - [Future in Malicious Code 2006 \(2006-08-05 17:43\)](#)
  - [DVD of the Weekend - The Final Cut \(2006-08-06 20:26\)](#)
  - [Malware Bot Families, Technology and Trends \(2006-08-07 00:43\)](#)
  - [JitterBugs - Covert Keyboard Communication Channels \(2006-08-09 05:27\)](#)
  - [Big Momma Knows Best \(2006-08-09 06:06\)](#)
  - [AOL's Search Leak User 4417749 Identified \(2006-08-10 00:21\)](#)
  - [Analyzing the Intelligence Analysts' Factors of Productivity \(2006-08-10 01:18\)](#)
  - [Malware Statistics on Social Networking Sites \(2006-08-10 02:11\)](#)

- [China's Internet Censorship Report 2006 \(2006-08-11 16:59\)](#)
- [Anti Satellite Weapons \(2006-08-12 03:01\)](#)
- [Bed Time Reading - Symbian OS Platform Security: Software Development Using the Symbian OS Security Architecture \(2006-08-12 03:21\)](#)
- [AOL's Search Queries Data Mined \(2006-08-16 06:38\)](#)
- [On the Insecurities of Sun Tanning \(2006-08-19 20:49\)](#)
- [North Korea's Strategic Developments and Financial Operations \(2006-08-20 00:15\)](#)
- [U.S Air Force on MySpace \(2006-08-22 19:14\)](#)
- [Virus Outbreak Response Time \(2006-08-22 19:41\)](#)
- [Cyber Terrorism Communications and Propaganda \(2006-08-22 20:39\)](#)
- [Face Recognition At Home \(2006-08-26 00:48\)](#)
- [Futuristic Warfare Technologies \(2006-08-26 01:27\)](#)
- [Microsoft's OneCare Penetration Pricing Strategy \(2006-08-26 14:17\)](#)
- [Steganography and Cyber Terrorism Communications \(2006-08-26 16:13\)](#)
- [Bed Time Reading - Spying on the Bomb \(2006-08-27 23:45\)](#)
- [Cyber War Strategies and Tactics \(2006-08-28 00:39\)](#)
- [September](#)
  - [The Walls and Lamps are Listening \(2006-09-02 00:13\)](#)
  - [The Biggest Military Hacks of All Time \(2006-09-02 00:21\)](#)
  - [Chinese Hackers Attacking U.S Department of Defense Networks \(2006-09-03 20:58\)](#)

- [Zero Day Initiative Upcoming Zero Day Vulnerabilities \(2006-09-04 21:03\)](#)
- [Stealth Satellites Developments Source Book \(2006-09-04 23:40\)](#)
- [Benefits of Open Source Intelligence - OSINT \(2006-09-05 00:49\)](#)
- [HP Spying on Board of Directors' Phone Records \(2006-09-06 17:33\)](#)
- [Hezbollah's use of Unmanned Aerial Vehicles - UAVs \(2006-09-06 19:36\)](#)
- [Google Hacking for Cryptographic Secrets \(2006-09-07 19:10\)](#)
- [Benchmarking and Optimising Malware \(2006-09-08 03:43\)](#)
- [Email Spam Harvesting Statistics \(2006-09-08 04:25\)](#)
- [A Study on The Value of Mobile Location Privacy \(2006-09-08 16:18\)](#)
- [The Freedom Tower - 11th September 2006 \(2006-09-11 20:57\)](#)
- [NSA's Terrorist Records Database \(2006-09-11 20:59\)](#)
- [Secret CIA Prisons \(2006-09-11 21:02\)](#)
- [Visualizing Enron's Email Communications \(2006-09-12 05:33\)](#)
- [Google Anti-Phishing Black and White Lists \(2006-09-13 02:08\)](#)
- [Testing Intrusion Prevention Systems \(2006-09-13 22:00\)](#)
- [Vulnerabilities in Emergency SMS Broadcasting \(2006-09-13 22:07\)](#)
- [Malware on Diebold Voting Machines \(2006-09-13 22:50\)](#)
- [Prosecuting Defectors and Appointing Insiders \(2006-09-13 23:14\)](#)

- [Internet PSYOPS - Psychological Operations \(2006-09-14 13:11\)](#)
- [Leaked Unmanned Aerial Vehicle Photo of Taliban Militants \(2006-09-18 16:03\)](#)
- [Cyber Intelligence - CYBERINT \(2006-09-18 21:16\)](#)
- [Examining Internet Privacy Policies \(2006-09-18 21:59\)](#)
- [Results of the Cyber Storm Exercise \(2006-09-18 22:01\)](#)
- [Banking Trojan Defeating Virtual Keyboards \(2006-09-19 13:15\)](#)
- [Soviet Propaganda Posters During the Cold War \(2006-09-22 02:06\)](#)
- [Airport Security Flash Game \(2006-09-22 02:31\)](#)
- [Interesting Anti-Phishing Projects \(2006-09-22 02:56\)](#)
- [Hezbollah's DNS Service Providers from 1998 to 2006 \(2006-09-22 03:18\)](#)
- [HP's Surveillance Methods \(2006-09-25 02:00\)](#)
- [Able Danger's Intelligence Unit Findings Rejected \(2006-09-25 02:44\)](#)
- [Terrorism and Response 1990-2005 \(2006-09-25 03:56\)](#)
- [Media Censorship in China - FAQ \(2006-09-27 12:23\)](#)
- [Afterlife Data Privacy \(2006-09-27 13:36\)](#)
- [Anti-Counterfeiting Technologies \(2006-09-28 00:47\)](#)
- [NSA Mind Control and PSYOPS \(2006-09-28 01:02\)](#)
- [Satellite Imagery of Secret or Sensitive Locations \(2006-09-28 02:12\)](#)
- [Government Data Mining Programs - Interactive \(2006-09-28 02:56\)](#)
- [October](#)



- [Mark Hurd on HP's Surveillance and Disinformation \(2006-10-04 18:22\)](#)
- [Filtering "Good Girls" and IM Threats \(2006-10-05 15:21\)](#)
- [Terrorist Letters and Internet Intentions \(2006-10-05 15:49\)](#)
- [SCADA Security Incidents and Critical Infrastructure Insecurities \(2006-10-05 16:21\)](#)
- [Automated SEO Spam Generation \(2006-10-12 13:27\)](#)
- [The Insider's Guide to Georgia-Russia Espionage Case \(2006-10-12 14:26\)](#)
- [Luxury Vehicles on Demand \(2006-10-12 15:02\)](#)
- [China Targeting U.S Satellite - Laser Ranging or Demonstration of Power? \(2006-10-12 15:24\)](#)
- [The History and Future of U.S. Military Satellite Communication Systems \(2006-10-12 17:32\)](#)
- [North Korea's Nuclear Testing Roundup \(2006-10-12 17:53\)](#)
- [The Return on Investment of Blogging \(2006-10-12 19:17\)](#)
- [Hunting the Hacker - Documentary \(2006-10-14 20:14\)](#)
- [North Korea's Wake-up Call \(2006-10-15 00:26\)](#)
- [Observing and Analyzing Botnets \(2006-10-16 01:15\)](#)
- [CIA's In-Q-Tel Investments Portfolio \(2006-10-16 01:50\)](#)
- [Registered Sex Offenders on MySpace \(2006-10-17 00:00\)](#)
- [The Stereotyped Beauty Model \(2006-10-18 20:39\)](#)
- [A Cost-Benefit Analysis of Cyber Terrorism \(2006-10-18 21:01\)](#)
- [Detecting Malware Time Bombs with Virtual Machines \(2006-10-24 12:42\)](#)

- [China's Information Security Market \(2006-10-24 12:56\)](#)
- [The Surveillance System About to Get Overloaded \(2006-10-24 14:19\)](#)
- [What are you Looking at? \(2006-10-26 15:13\)](#)
- [Ms. Dewey on Microsoft and Security \(2006-10-26 15:31\)](#)
- [ShotSpotter - Gunshot Sensors Network \(2006-10-26 15:55\)](#)
- [Real-Time Spam Outbreak Statistics \(2006-10-28 20:57\)](#)
- [Face Recognition on 3G Cell Phones \(2006-10-29 00:41\)](#)
- [Greetings Professor Falken \(2006-10-29 01:43\)](#)
- [Fake Search Warrant Generator \(2006-10-30 17:40\)](#)
- [November](#)
  - [Proof of Concept Symbian Malware Courtesy of the Academic World \(2006-11-01 19:03\)](#)
  - [FAS's Immune Attack Game \(2006-11-01 20:09\)](#)
  - [Delicious Information Warfare - Friday \(2006-11-03 04:04\)](#)
  - [The Blogosphere and Splogs \(2006-11-07 23:38\)](#)
  - [All Your Electromagnetic Transmissions Are Belong To Us \(2006-11-09 17:07\)](#)
  - [The Nuclear Grabber Toolkit \(2006-11-09 21:32\)](#)
  - [Bill Gates on Traffic Acquisition and Internet Bubbles \(2006-11-13 01:23\)](#)
  - [Jihadi PSYOPS - CIA Attacks on Terrorist Websites \(2006-11-13 03:42\)](#)
  - [U.S No-Fly-List Enforced at Deutsche Bank NYC \(2006-11-14 02:51\)](#)
  - [Satellite Imagery Trade-offs \(2006-11-14 03:37\)](#)
  - [Widener University Forensics Course \(2006-11-14 04:02\)](#)

- [London's Police Experimenting with Head-Mounted Surveillance Cameras \(2006-11-20 20:35\)](#)
- [How to Tell if Someone's Lying to You \(2006-11-27 04:31\)](#)
- [To Publish a Privacy Policy or Not to Publish a Privacy Policy \(2006-11-27 04:45\)](#)
- [Global Map of Security Incidents and Terrorist Events \(2006-11-27 05:39\)](#)
- [How to Fake Fingerprints \(2006-11-27 06:24\)](#)
- [Video of Birds Attacking an Unmanned Aerial Vehicle \(UAV\) \(2006-11-29 17:13\)](#)
- [CIA Personality Quiz \(2006-11-29 17:28\)](#)
- [A Movie About Trusted Computing \(2006-11-30 18:10\)](#)
- [A Chart of Personal Data Security Breaches 2005-2006 \(2006-11-30 18:31\)](#)
- [December](#)
  - [Symantec's Invisible Burglar Game \(2006-12-07 15:45\)](#)
  - [Symantec's Invisible Burglar Game \(2006-12-07 16:46\)](#)